P-330W

802.11g Secure Wireless Internet Sharing Router

User's Guide

Version 1.0
May 2005

ZyXEL
Unleash Networking Power

Copyright

Copyright © 2005 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Notice 1

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Certifications

Go to www.us.zyxel.com

1. Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
2. Select the certification you wish to view from this page

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind of character to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Safety Warnings

1. To reduce the risk of fire, use only No. 26 AWG or larger telephone wire.
2. Do not use this product near water, for example, in a wet basement or near a swimming pool.
3. Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightening.

This product has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

Customer Support

Please have the following information ready when you contact customer support.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

METHOD LOCATION	SUPPORT E-MAIL SALES E-MAIL	TELEPHONE FAX	WEB SITE FTP SITE	REGULAR MAIL
NORTH AMERICA	support@zyxel.com	+1-800-255-4101 +1-714-632-0882	www.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
	sales@zyxel.com	+1-714-632-0858	ftp.us.zyxel.com	

Table of Contents

Copyright **2**

Federal Communications Commission (FCC) Interference Statement **3**

ZyXEL Limited Warranty **4**

Customer Support **5**

Preface **16**

Chapter 1
Getting to Know Your P-330W **18**

1.1 P-330W Internet Security Gateway Overview 18
1.2 P-330W Features 18
1.2.1 Physical Features 18
1.2.1.1 10/100M Auto-negotiating Ethernet/Fast Ethernet Interface(s) 18
1.2.1.2 Auto-crossover 10/100 Mbps Ethernet Interface(s) 18
1.2.1.3 4-Port Switch 18
1.2.1.4 Time and Date 19
1.2.1.5 Reset Button 19
1.2.2 Removable Antenna 19
1.2.3 Non-Physical Features 19
1.2.3.1 Firewall 19
1.2.3.2 802.11b Wireless LAN Standard 19
1.2.3.3 802.11g Wireless LAN Standard 20
1.2.3.4 Packet Filtering 20
1.2.3.5 Universal Plug and Play (UPnP) 20
1.2.3.6 PPPoE 20
1.2.3.7 PPTP Encapsulation 20
1.2.3.8 Dynamic DNS Support 20
1.2.3.9 Network Address Translation (NAT) 21
1.2.3.10 Port Forwarding 21
1.2.3.11 DHCP (Dynamic Host Configuration Protocol) 21
1.2.3.12 Logging and Tracing 21
1.2.3.13 Wireless Association List 21
1.3 Applications for the P-330W 21
1.3.1 Secure Broadband Internet Access via Cable or DSL Modem 21

1.3.2 Internet Access Application 22

Chapter 2
Introducing the Web Configurator 24

2.1 Web Configurator Overview 24
2.2 Accessing the P-330W Web Configurator 24
2.2.0.1 Resetting the P-330W 24
2.2.1 Navigating the P-330W Web Configurator 25
2.2.2 Navigation Panel 25

Chapter 3
Wizard Setup 28

3.1 Wizard Setup Overview 28
3.2 Wizard Setup: Screen 2 28
3.2.1 DHCP Client 28
3.2.2 Static IP 28
3.2.3 PPPoE Encapsulation 29
3.2.4 PPTP Encapsulation 30
3.2.5 L2TP Encapsulation 31
3.3 Wizard Setup: Screen 3 32
3.4 Wizard Setup: Screen 4 33
3.4.1 No Encryption 34
3.4.2 WEP Encryption 34
3.4.3 WPA (TKIP) 35
3.4.4 WPA2 (AES) 35
3.4.5 WPA2 Mixed 36
3.5 Basic Setup Complete 37

Chapter 4
System Screens 38

4.1 Setup Wizard 38
4.2 Operation Mode 38
4.3 LAN Overview 39
4.3.1 DHCP Setup 40
4.3.2 IP Pool Setup 40
4.3.3 System DNS Servers 40
4.3.4 LAN TCP/IP 40
4.3.5 Factory LAN Defaults 40
4.3.6 IP Address and Subnet Mask 40
4.3.7 Configuring IP 40
4.4 Configuring Password 41
4.5 Status Screen 42

Chapter 5
Wireless 44

5.1 Wireless LAN Overview 44
5.1.1 IBSS 44
5.1.2 BSS 44
5.1.3 ESS 45
5.1.4 RTS/CTS 46
5.2 Configuring Wireless 47
5.3 Basic Settings 47
5.4 Wireless Advanced Settings 49
5.4.1 Authentication 49
5.4.2 Preamble Type 50
5.5 Wireless Security Overview 51
5.6 Security Parameters Summary 53
5.6.1 WEP Overview 53
5.6.2 Data Encryption 53
5.6.3 Configuring WEP Encryption 53
5.6.4 Introduction to WPA 56
5.6.4.1 User Authentication 56
5.6.4.2 Encryption 56
5.6.4.3 WPA-PSK Application Example 57
5.6.5 Introduction to WPA2 57
5.6.6 Configuring WPA-PSK Authentication 57
5.6.7 Introduction to RADIUS 59
5.6.7.1 Types of RADIUS Messages 59
5.6.7.2 Access-Challenge 59
5.6.7.3 Accounting-Request 59
5.6.7.4 Accounting-Response 59
5.6.7.5 EAP Authentication Overview 60
5.6.7.6 WPA with RADIUS Application Example 60
5.6.8 Configuring WPA Authentication 61
5.7 Wireless Trusted Stations 63

Chapter 6
Advanced Options 66

6.1 Access Control 66
6.2 Dynamic DNS 67
6.3 Configuring Dynamic DNS 68
6.4 DMZ 69
6.5 Virtual Servers (Port Forwarding) 69
6.5.0.1 Configuring Servers Behind SUA (Example) 70
6.5.1 Configuring Virtual Servers 71
6.6 ALG 72

6.7 WAN Port 73
6.7.1 Static IP Encapsulation 73
6.7.2 DHCP IP Encapsulation 75
6.7.3 PPPoE Encapsulation 76
6.7.4 PPTP Encapsulation 78
6.7.5 L2TP Encapsulation 80
6.8 Ping 82
6.9 DoS Setting 83
6.10 Diagnostics 84

Chapter 7
Administrator Options 86

7.1 Remote Management 86
7.2 Configuration Screen 86
7.2.1 Backup Configuration 87
7.2.2 Restore Configuration 87
7.2.3 Back to Factory Defaults 88
7.3 Logs 88
7.4 IP Filtering 89
7.5 MAC Filtering 90
7.6 URL Filtering 91
7.7 Statistics 92
7.8 Time Zone Setting 92
7.9 Upgrade Firmware 93

Appendix A
PPPoE 96

Appendix B
PPTP 98

Appendix C
Setting up Your Computer's IP Address 102

Appendix D
Wireless LAN and IEEE 802.11 114

Appendix E
Wireless LAN With IEEE 802.1x 118

Appendix F
Types of EAP Authentication 120

Appendix G
Antenna Selection and Positioning Recommendation 122

List of Figures

Figure 1 Secure Internet Access via Cable, DSL or Wireless Modem 22
Figure 2 Internet Access Application Example 22
Figure 3 The MAIN MENU Screen of the Web Configurator 25
Figure 4 Wizard 2: DHCP Client Encapsulation 28
Figure 5 Wizard 2: Static IP Encapsulation 29
Figure 6 Wizard 2: PPPoE Encapsulation 30
Figure 7 Wizard 2: PPTP Encapsulation 31
Figure 8 Wizard 2: L2TP Encapsulation 32
Figure 9 Wizard 3: Wireless LAN Basic Setup 33
Figure 10 Wizard 4: Wireless LAN Setup: WEP Security 34
Figure 11 Wizard 4: Wireless LAN Setup: WPA Security 35
Figure 12 Wizard 4: Wireless LAN Setup: WPA2 Security 36
Figure 13 Wizard 4: Wireless LAN Setup: WPA2 Security 37
Figure 14 System Screen Menu Options 38
Figure 15 Operation Mode Setup 39
Figure 16 LAN IP Setup 41
Figure 17 Password 42
Figure 18 Status 43
Figure 19 IBSS (Ad-hoc) Wireless LAN 44
Figure 20 Basic Service set 45
Figure 21 Extended Service Set 46
Figure 22 RTS/CTS 46
Figure 23 The Wireless Options Screen 47
Figure 24 Wireless: Basic Settings 48
Figure 25 WEP Authentication Steps 49
Figure 26 Wireless: Advanced Settings 50
Figure 27 P-330W Wireless Security Levels 51
Figure 28 Wireless Security Setup: No Security 52
Figure 29 Wireless Security Setup: WEP Encryption 54
Figure 30 Wireless Security Setup: WEP Encryption 55
Figure 31 WPA - PSK Authentication 57
Figure 32 Wireless Security Setup: WPA-PSK 58
Figure 33 EAP Authentication 60
Figure 34 WPA with RADIUS Application Example 61
Figure 35 Wireless Security Setup: WPA With RADIUS 62
Figure 36 Wireless: Trusted Stations MAC Address Filter 64

Figure 37 The Advanced Menu Options 66
Figure 38 Advanced: Access Control 67
Figure 39 Advanced: Dynamic DNS 68
Figure 40 Advanced: DMZ 69
Figure 41 Multiple Servers Behind NAT Example 71
Figure 42 Advanced: Virtual Servers 71
Figure 43 Advanced: ALG 73
Figure 44 Advanced: WAN Static IP Encapsulation 74
Figure 45 Advanced: WAN DHCP IP Encapsulation 75
Figure 46 Advanced: WAN PPPoE Encapsulation 77
Figure 47 Advanced: WAN PPTP Encapsulation 79
Figure 48 Advanced: WAN L2TP Encapsulation 81
Figure 49 Advanced: Ping 83
Figure 50 Advanced: DoS 84
Figure 51 Advanced: Diagnostic 85
Figure 52 Administrator: Remote Management 86
Figure 53 Administrator: Configuration File 87
Figure 54 Temporarily Disconnected 88
Figure 55 Administrator: Logs 89
Figure 56 Administrator: IP Filtering 90
Figure 57 Administrator: MAC Filtering 91
Figure 58 Administrator: URL Filtering 92
Figure 59 Administrator: Time Zone Setting 93
Figure 60 Administrator: Upgrade Firmware 94
Figure 61 Upload Warning 94
Figure 62 Network Temporarily Disconnected 95
Figure 63 Single-Computer per Router Hardware Configuration 97
Figure 64 P-330W as a PPPoE Client 97
Figure 65 Transport PPP frames over Ethernet 98
Figure 66 PPTP Protocol Overview 99
Figure 67 Example Message Exchange between Computer and an ANT 100
Figure 68 WIndows 95/98/Me: Network: Configuration 103
Figure 69 Windows 95/98/Me: TCP/IP Properties: IP Address 104
Figure 70 Windows 95/98/Me: TCP/IP Properties: DNS Configuration 105
Figure 71 Windows XP: Start Menu 106
Figure 72 Windows XP: Control Panel 106
Figure 73 Windows XP: Control Panel: Network Connections: Properties 107
Figure 74 Windows XP: Local Area Connection Properties 107
Figure 75 Windows XP: Advanced TCP/IP Settings 108
Figure 76 Windows XP: Internet Protocol (TCP/IP) Properties 109
Figure 77 Macintosh OS 8/9: Apple Menu 110
Figure 78 Macintosh OS 8/9: TCP/IP 111
Figure 79 Macintosh OS X: Apple Menu 111

Figure 80 Macintosh OS X: Network 112
Figure 81 Peer-to-Peer Communication in an Ad-hoc Network 115
Figure 82 ESS Provides Campus-Wide Coverage 116
Figure 83 Sequences for EAP MD5–Challenge Authentication 119

List of Tables

Table 1 IEEE 802.11b 19
Table 2 IEEE 802.11g 20
Table 3 Screens Summary 26
Table 4 Wizard 2: Ethernet Encapsulation 29
Table 5 Wizard 2: PPPoE Encapsulation 30
Table 6 Wizard 2: PPTP Encapsulation 31
Table 7 Wizard 2: L2TP Encapsulation 32
Table 8 Wizard 3: Wireless LAN Basic Setup 33
Table 9 Wizard 4: Wireless LAN Setup: WEP Security 34
Table 10 Wizard 4: Wireless LAN Setup: WPA Security 35
Table 11 Wizard 4: Wireless LAN Setup: WPA2 Security 36
Table 12 Wizard 4: Wireless LAN Setup: WPA2 Security 37
Table 13 System General Setup 39
Table 14 LAN IP Setup 41
Table 15 Password 42
Table 16 Status 43
Table 17 Wireless: Basic Settings 48
Table 18 Wireless: Advanced Settings 50
Table 19 Wireless Security Setup: No Security 52
Table 20 Wireless Security Relational Matrix 53
Table 21 Wireless Security Setup: Static WEP Encryption 54
Table 22 Wireless Security Setup: WEP Encryption 55
Table 23 Wireless Security Setup: WPA-PSK 58
Table 24 Wireless Security Setup: WPA 62
Table 25 Wireless: Trusted Stations MAC Address Filter 64
Table 26 Advanced: Access Control 67
Table 27 Advanced: Dynamic DNS 68
Table 28 Advanced: DMZ 69
Table 29 Services and Port Numbers 70
Table 30 Advanced: Virtual Servers 71
Table 31 Advanced: ALG 73
Table 32 Advanced: WAN Static IP Encapsulation 74
Table 33 Advanced: WAN DHCP IP Encapsulation 75
Table 34 PPPoE Encapsulation 77
Table 35 Advanced: WAN PPTP Encapsulation 79
Table 36 Advanced: WAN L2PTP Encapsulation 81

Table 37 Advanced: Ping 83
Table 38 Advanced: DoS 84
Table 39 Advanced: Diagnostic 85
Table 40 Administrator: Remote Management 86
Table 41 Maintenance Restore Configuration 87
Table 42 Administrator: Remote Management 89
Table 43 Administrator: IP Filtering 90
Table 44 Administrator: MAC Filtering 91
Table 45 Administrator: URL Filtering 92
Table 46 Administrator: Time Zone Setting 93
Table 47 Administrator: Upgrade Firmware 94
Table 48 Comparison of EAP Authentication Types 121

Preface

Congratulations on your purchase of the P-330W, 802.11g Secure Wireless Internet Sharing Router. This manual is designed to guide you through the configuration of your P-330W for its various applications.

This manual may refer to the P-330W or 802.11g Secure Wireless Internet Sharing Router as the router.

About This User's Guide

This User's Guide is designed to guide you through the configuration of your P-330W using the web configurator(GUI). The web configurator parts of this guide contain background information on features configurable by web configurator.

Related Documentation

- Support Disk

  Refer to the included CD for support documents.

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. They contain connection information and instructions on getting started.

- ZyXEL Glossary and Web Site

  Please refer to www.us.zyxel.com for an online glossary of networking terms and additional support documentation.

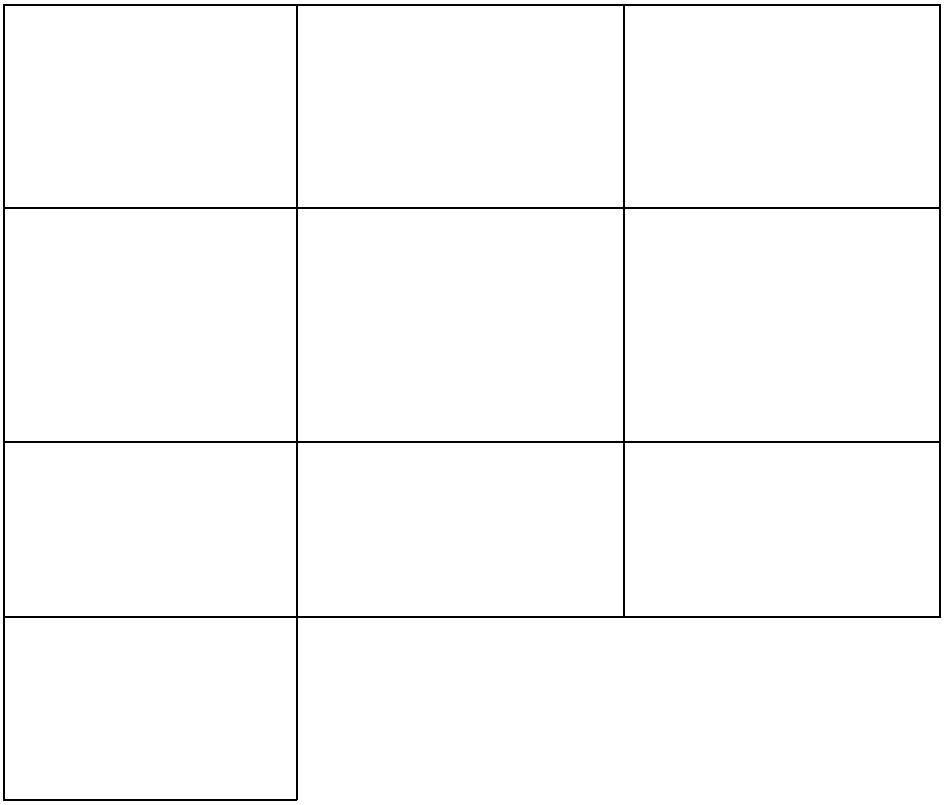
User Guide Feedback

Help us help you! E-mail all User Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com

Syntax Conventions

- "Enter" means for you to type one or more characters. "Select" or "Choose" means for you to use one predefined choices.
- Mouse action sequences are denoted using a comma. For example, "click the Apple icon, **Control Panels** and then **Modem**" means first click the Apple icon, then point your mouse pointer to **Control Panels** and then click **Modem**.
- For brevity's sake, we will use "e.g.," as a shorthand for "for instance", and "i.e.," for "that is" or "in other words" throughout this manual.

Graphics Icons Key



CHAPTER 1
Getting to Know Your P-330W

This chapter introduces the main features and applications of the P-330W.

1.1 P-330W Internet Security Gateway Overview

The P-330W is the ideal secure gateway for all data passing between the Internet and LAN's.

By integrating NAT, firewall, wireless access point and 4-port switch, ZyXEL's P-330W is a complete security solution that protects your Intranet and efficiently manages data traffic on your network.

The embedded web configurator is easy to operate.

1.2 P-330W Features

The following sections describe P-330W features..

1.2.1 Physical Features

1.2.1.1 10/100M Auto-negotiating Ethernet/Fast Ethernet Interface(s)

This auto-negotiation feature allows the P-330W to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

1.2.1.2 Auto-crossover 10/100 Mbps Ethernet Interface(s)

These interfaces automatically adjust to either a crossover or straight-through Ethernet cable.

1.2.1.3 4-Port Switch

A combination of switch and router makes your P-330W a cost-effective and viable network solution. You can add up to four computers to the P-330W without the cost of a hub. Add more than four computers to your LAN by using a hub.

1.2.1.4 Time and Date

The P-330W allows you to get the current time and date from an external server when you turn on your P-330W. You can also set the time manually.

1.2.1.5 Reset Button

The P-330W reset button is built into the rear panel. You can use this button to either cause the P-330W to reboot, or to reset the P-330W to factor defaults. Use this button to restore the factory default password to 1234; IP address to 192.168.1.1, subnet mask to 255.255.255.0 and DHCP server enabled with a pool of 32 IP addresses starting at 192.168.1.33. For further instructions see Chapter 2.

1.2.2 Removable Antenna

The P-330W antenna uses an RP-SMA connection to attach to the P-330W. It is possible to remove the antenna and replace it with another antenna that offers different performance characteristics.

1.2.3 Non-Physical Features

1.2.3.1 Firewall

The P-330W is a home firewall with DoS (Denial of Service) protection. By default, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN.

1.2.3.2 802.11b Wireless LAN Standard

The P-330W, complies with the 802.11b wireless standard.

The 802.11b data rate and corresponding modulation techniques are as follows. The modulation technique defines how bits are encoded onto radio waves.

Table 1 IEEE 802.11b

	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)

1.2.3.3 802.11g Wireless LAN Standard

The P-330W, complies with the 802.11g wireless standard and is also fully compatible with the 802.11b standard. This means an 802.11b radio card can interface directly with an 802.11g device (and vice versa) at 11 Mbps or lower depending on range. 802.11g has several intermediate rate steps between the maximum and minimum data rates. The 802.11g data rate and modulation are as follows:

Table 2 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

1.2.3.4 Packet Filtering

The packet filtering mechanism blocks unwanted traffic from entering/leaving your network.

1.2.3.5 Universal Plug and Play (UPnP)

Using the standard TCP/IP protocol, the P-330W and other UPnP enabled devices can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.

1.2.3.6 PPPoE

PPPoE facilitates the interaction of a host with an Internet modem to achieve access to high-speed data networks via a familiar "dial-up networking" user interface.

1.2.3.7 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using a TCP/IP-based network.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet. The P-330W supports one PPTP server connection at any given time.

1.2.3.8 Dynamic DNS Support

With Dynamic DNS (Domain Name System) support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service with a Dynamic DNS service provider.

1.2.3.9 Network Address Translation (NAT)

Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).

1.2.3.10 Port Forwarding

Use this feature to forward incoming service requests to a server on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server.

1.2.3.11 DHCP (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) allows the individual client computers to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The P-330W has built-in DHCP server capability, enabled by default, which means it can assign IP addresses, an IP default gateway and DNS servers to all systems that support the DHCP client.

1.2.3.12 Logging and Tracing

- System Logs
- Wireless Logs
- DoS Logs

1.2.3.13 Wireless Association List

With the Wireless Association List, you can see the list of the wireless stations that are currently using the P-330W to access your wired network.

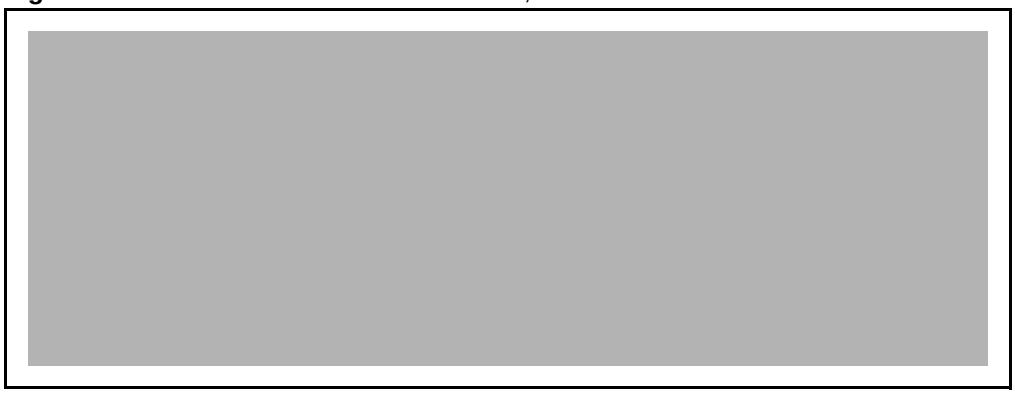
1.3 Applications for the P-330W

Here are some examples of what you can do with your P-330W.

1.3.1 Secure Broadband Internet Access via Cable or DSL Modem

You can connect a cable modem, DSL or wireless modem to the P-330W for broadband Internet access via an Ethernet or a wireless port on the modem. The P-330W guarantees not only high speed Internet access, but secure internal network protection and traffic management as well.

Figure 1 Secure Internet Access via Cable, DSL or Wireless Modem



1.3.2 Internet Access Application

Add a wireless LAN to your existing network without expensive network cables. Wireless stations can move freely anywhere in the coverage area and use resources on the wired network.

Figure 2 Internet Access Application Example

CHAPTER 2
Introducing the Web Configurator

This chapter describes how to access the P-330W web configurator and provides an overview of its screens.

2.1 Web Configurator Overview

The embedded web configurator allows you to manage the P-330W from anywhere through a browser such as Microsoft Internet Explorer or Netscape Navigator. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions with JavaScript enabled. It is recommended that you set your screen resolution to 1024 by 768 pixels. The screens you see in the web configurator may vary somewhat from the ones shown in this document due to differences between individual P-330W models or firmware versions.

2.2 Accessing the P-330W Web Configurator

1. Make sure your P-330W hardware is properly connected and prepare your computer/ computer network to connect to the P-330W (refer to the *Quick Start Guide*).
2. Launch your web browser.
3. Type "192.168.1.1" as the URL.
4. Type “admin” as the User Name
5. Type "1234" (default) as the password.
6. Click **OK** to login.

You should now see the **MAIN MENU** screen)

2.2.0.1 Resetting the P-330W

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the P-330W to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to “1234”.

2.2.0.1.1 Procedure To Use The Reset Button

1. Make sure the **PWR** LED is on (not blinking).
2. Press the **RESET** button for approximately ten seconds or until the **PWR** LED begins to blink and then release it. When the **PWR** LED begins to blink, the defaults have been restored and the P-330W restarts. (If you press the **RESET** button for less than 5 seconds, the P-330W will reboot, but will not reset the configuration).

2.2.1 Navigating the P-330W Web Configurator

The following summarizes how to navigate the web configurator from the **SITE MAP** screen.

- Click **SETUP WIZARD** for initial configuration including general setup, **Wireless LAN Setup**, ISP parameters for Internet Access and WAN IP/DNS Server/MAC address assignment.
- Click a link under **WIRELESS** to configure wireless settings.
- Click a link under **ADVANCED** to configure advanced P-330W features.
- Click **LOGOUT** at any time to exit the web configurator.
- Click **ADMINISTRATOR** to view information about your P-330W or upgrade configuration/firmware files. Administrator includes **Statistics**, **Remote Management**, **Upgrade Firmware**, **Config File** (Backup, Restore, Defaults) and **Time Zone Settings**.

Figure 3 The MAIN MENU Screen of the Web Configurator

2.2.2 Navigation Panel

After you log in, use the sub-menus on the navigation panel to configure P-330W features.

The following table describes the sub-menus.

Table 3 Screens Summary

LINK	TAB	FUNCTION
SETUP WIZARD		Use these screens for initial configuration including general setup, Wireless LAN setup, ISP parameters for Internet Access and WAN IP/DNS Server/MAC address assignment.
OPERATION MODE		Use this screen to switch the P-330W between gateway, bridge, and wireless client mode.
LAN		Use this screen to configure you LAN, including default IP address of the P-330W, LAN DHCP, and viewing current DHCP clients.
PASSWORD		Use this screen to change your password.
STATUS		This screen contains administrative and system-related information.
WIRELESS	Basic Settings	Use this screen to configure the wireless LAN.
	Advanced Settings	Use this screen to configured advanced wireless system behavior.
	Security	Use this screen to configure wireless encryption and authorization settings.
	Trusted Stations	Use this screen to set up MAC address filtering for WLAN clients.
ADVANCED	Access Control	Use this screen to set up packet filtering policies.
	Dynamic DNS	Use this screen to configure dynamic DNS service settings.
	DMZ	Use this screen to isolate a specific device from the rest of the network.
	Virtual Servers	Use this screen to configure servers behind the P-330W.
	Special Applications	Use this screen to change your P-330W's trigger port settings.
	ALG	Use this screen to selection which applications require special NAT rules.
	WAN Port	Use this screen to change your P-330W's WAN ISP settings.
	Ping	Use this screen to verify network connectivity.
	DoS Settings	Use this screen to configure Denial of Service settings.
	Diagnostics	Use this page to look up DNS information.
Administrator	Remote Management	Use this page to allow remote clients to manage the P-330W.
	Config File	Use this screen to backup and restore the configuration or reset the factory defaults to your P-330W.
	Logs	Use this screen to change your P-330W's log settings and to view the logs for the categories that you selected.
	IP Filtering	Use this page to configure a list of IP addresses that the router will not allow traffic to or from.
	MAC Filtering	Use the MAC filter screen to configure the P-330W to block access to devices or block the devices from accessing the P-330W.
	URL Filtering	This screen allows you to block sites containing certain web sites based on their URL.

Table 3 Screens Summary

LINK	TAB	FUNCTION
Administrator	Statistics	This screen contains administrative and system-related information.
	Time Zone Setting	Use this screen to change your P-330W's time and date or enable NTP server use.
	Upgrade Firmware	Use this screen to upload firmware to your P-330W.
LOG OUT		Click this label to exit the web configurator.

CHAPTER 3
Wizard Setup

This chapter provides information on the Wizard Setup screens in the web configurator.

3.1 Wizard Setup Overview

The web configurator's setup wizard helps you configure your device to access the Internet. The second screen has five variations depending on what encapsulation type you use. Refer to your ISP checklist in the *Quick Start Guide* to know what to enter in each field. Leave a field blank if you don't have that information.

The fifth wizard screen varies according to the type of encapsulation that you select in the third wizard screen.

3.2 Wizard Setup: Screen 2

The P-330W offers five choices of encapsulation. They are **DHCP Client**, **Static IP**, **PPP over Ethernet, L2TP** or **PPTP**.

3.2.1 DHCP Client

Choose **DHCP Client** when the WAN port is used as regular Ethernet and your ISP assigns you an IP address via DHCP.

Figure 4 Wizard 2: DHCP Client Encapsulation

3.2.2 Static IP

Choose Static IP when the WAN port is used as regular Ethernet and your ISP assigns you a fixed IP address.

Figure 5 Wizard 2: Static IP Encapsulation

The following table describes the labels in this screen.

Table 4 Wizard 2: Ethernet Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
IP Address	The fixed IP address should be in the same subnet as your broadband modem or router. This should be provided to you by your ISP
Subnet Mask	Enter a **Subnet Mask** appropriate to your network.
Default Gateway	Enter the **Gateway IP Address** of the neighboring device, if you know it. If you do not, leave the Gateway IP Address field blank.
DNS	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. Enter your **DNS Server** IP address here.
Cancel	Click **Cancel** to abort the setup wizard.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.

3.2.3 PPPoE Encapsulation

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) draft standard specifying how a host personal computer interacts with a broadband modem (for example DSL, cable, wireless, etc.) to achieve access to high-speed data networks.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for instance, Radius). For the user, PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

One of the benefits of PPPoE is the ability to let end users access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for specific users.

Operationally, PPPoE saves significant effort for both the subscriber and the ISP/carrier, as it requires no specific configuration of the broadband modem at the subscriber's site.

By implementing PPPoE directly on the P-330W (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the P-330W does that part of the task. Furthermore, with NAT, all of the LAN's computers will have Internet access.

Refer to the appendix for more information on PPPoE.

Figure 6 Wizard 2: PPPoE Encapsulation

The following table describes the labels in this screen.

Table 5 Wizard 2: PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameter for Internet Access	
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Cancel	Click **Cancel** to abort the setup wizard.
Next	Click **Next** to continue.
Back	Click **Back** to return to the previous screen.

3.2.4 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables transfers of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet.

Refer to the appendix for more information on PPTP.

Figure 7 Wizard 2: PPTP Encapsulation

The following table describes the fields in this screen

Table 6 Wizard 2: PPTP Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
IP Address	Type the (static) IP address assigned to you by your ISP.
IP Subnet Mask	Type the subnet mask assigned to you by your ISP.
Server IP Address	Type the IP address of the PPTP server.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Cancel	Click **Cancel** to abort the setup wizard.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.

3.2.5 L2TP Encapsulation

Layer Two Tunneling Protocol (L2TP) is a network protocol that enables transfers of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

Figure 8 Wizard 2: L2TP Encapsulation

The following table describes the fields in this screen

Table 7 Wizard 2: L2TP Encapsulation

LABEL	DESCRIPTION
Attain IP Automatically	Select this if your ISP automatically assigns you an IP Address.
Set IP Manually	Select this if your ISP has assigned you a fixed IP address.
	Type the (static) IP address assigned to you by your ISP.
IP Subnet Mask	Type the subnet mask assigned to you by your ISP.
Server IP Address	Type the IP address of the L2TP server.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Cancel	Click **Cancel** to abort the setup wizard.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.

3.3 Wizard Setup: Screen 3

Set up the basics of your wireless LAN using the third wizard screen.

Figure 9 Wizard 3: Wireless LAN Basic Setup

The following table describes the labels in this screen.

Table 8 Wizard 3: Wireless LAN Basic Setup

LABEL	DESCRIPTION
Band	Choose the operating mode of your wireless access point. **2.4Ghz (B+G)** offers the greatest compatibility. **2.4 GHz (B)** will only allow 802.11b clients to connect to the wireless LAN. **2.4 GHz (G)** will only allow 802.11g clients to connect to the wireless LAN.
SSID	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the P-330W, make sure all wireless stations use the same SSID in order to access the network.
Channel Number	To manually set the P-330W to use a channel, select a channel from the drop-down list box.
Disable Access Point	Select this check box to disable the wireless LAN capabilities of your P-330W.
Cancel	Click **Cancel** to abort the setup wizard.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.

3.4 Wizard Setup: Screen 4

There are 5 different versions of this page depending on what method of encryption you want to enable on your wireless LAN.

3.4.1 No Encryption

Choose **None** to allow the WLAN to operate without encryption. Warning: With no encryption enabled anyone will be able to access your network and view any data you send over the wireless LAN.

3.4.2 WEP Encryption

Choose **WEP** to setup WEP Encryption parameters.

Figure 10 Wizard 4: Wireless LAN Setup: WEP Security

The following table describes the labels in this screen.

Table 9 Wizard 4: Wireless LAN Setup: WEP Security

LABEL	DESCRIPTION
Key Length	Select **64-bit WEP** or **128-bit WEP** data encryption.
Key Format	Select ASCII in order to enter ASCII characters as the WEP keys. Select Hex to enter hexadecimal characters as the WEP keys.
Default Tx Key	This key refers to which key below will be used as the default key.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the P-330W and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one key, only one key can be activated at any one time. The default key is key 1.

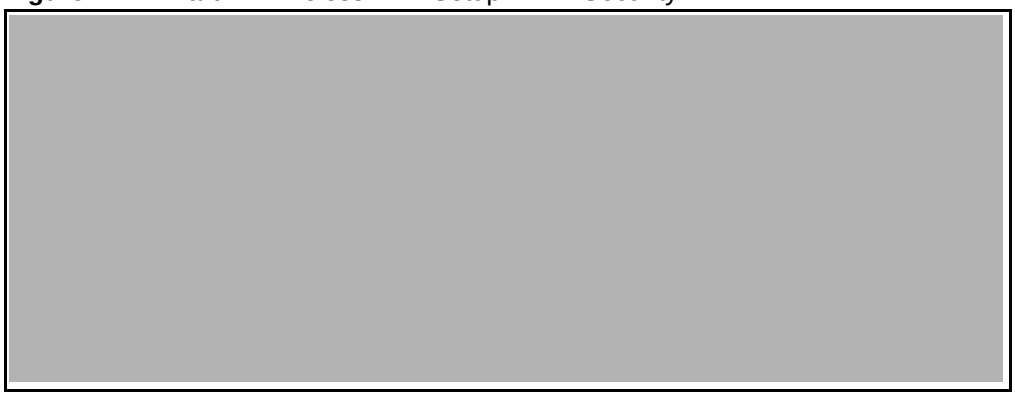
Table 9 Wizard 4: Wireless LAN Setup: WEP Security

LABEL	DESCRIPTION
Cancel	Click **Cancel** to abort the setup wizard.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.

3.4.3 WPA (TKIP)

Choose **WPA (TKIP)** security in the Wireless LAN Setup screen to set up a **Pre-Shared Key** using TKIP encryption.

Figure 11 Wizard 4: Wireless LAN Setup: WPA Security



The following table describes the labels in this screen.

Table 10 Wizard 4: Wireless LAN Setup: WPA Security

LABEL	DESCRIPTION
WPA Format	You can choose to enter the pre-shared key manually in HEX format or use a passphrase. Note, many client devices only allow entry via passphrase.
Pre-Shared Key	For Passphrase: Type from 8 to 63 case-sensitive ASCII characters. For HEX: Type a 64 character hex key.
Cancel	Click **Cancel** to abort the setup wizard.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.

3.4.4 WPA2 (AES)

Choose **WPA2 (AES)** security in the Wireless LAN Setup screen to set up a **Pre-Shared Key** using AES encryption.

Figure 12 Wizard 4: Wireless LAN Setup: WPA2 Security

The following table describes the labels in this screen.

Table 11 Wizard 4: Wireless LAN Setup: WPA2 Security

LABEL	DESCRIPTION
WPA Format	You can choose to enter the pre-shared key manually in HEX format or use a passphrase. Note, many client devices only allow entry via passphrase.
Pre-Shared Key	For Passphrase: Type from 8 to 63 case-sensitive ASCII characters. For HEX: Type a 64 character hex key.
Cancel	Click **Cancel** to abort the setup wizard.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.

3.4.5 WPA2 Mixed

Choose **WPA2 Mixed** security in the Wireless LAN Setup screen to set up a **Pre-Shared Key** using both TKIP and AES encryption. This allows both WPA and WPA2 clients to connect.

Figure 13 Wizard 4: Wireless LAN Setup: WPA2 Security

The following table describes the labels in this screen.

Table 12 Wizard 4: Wireless LAN Setup: WPA2 Security

LABEL	DESCRIPTION
WPA Format	You can choose to enter the pre-shared key manually in HEX format or use a passphrase. Note, many client devices only allow entry via passphrase.
Pre-Shared Key	For Passphrase: Type from 8 to 63 case-sensitive ASCII characters. For HEX: Type a 64 character hex key.
Cancel	Click **Cancel** to abort the setup wizard.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.

3.5 Basic Setup Complete

Click **Finish** to complete the wizard setup and save your configuration.

Well done! You have successfully set up your P-330W to operate on your network and access the Internet

CHAPTER 4
System Screens

This chapter provides information on the options configurable from the main System screens.

Figure 14 System Screen Menu Options

4.1 Setup Wizard

See the *Setup Wizard* chapter for more information on this selection.

4.2 Operation Mode

Click **Operation Mode** to open the **Operation Mode** screen.

Figure 15 Operation Mode Setup

The following table describes the labels in this screen.

Table 13 System General Setup

LABEL	DESCRIPTION
Gateway	This is the standard operating mode. The P-330W takes on all the usual roles of a home router, including NAT, DHCP Server, and Firewall.
Bridge	Select this to turn your P-330W into a pure bridge, directly linking all computers on your network to the WAN. In this mode, you have no protection from Internet based threats.
Wireless ISP	In this mode, the wireless LAN is disabled and instead the wireless module is acts as a client to connect to a Wireless ISP. All the normal router functions are enabled.
Save	Click **Save** to save your changes back to the P-330W.
Reset	Click **Reset** to begin configuring this screen afresh.

4.3 LAN Overview

Local Area Network (LAN) is a shared communication system to which many computers are attached. The LAN screens can help you configure a LAN DHCP server, manage IP addresses, and partition your physical network into logical networks.

4.3.1 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the P-330W as a DHCP server or disable it. When configured as a server, the P-330W provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

4.3.2 IP Pool Setup

The P-330W is pre-configured with a pool of 33 IP addresses starting from 192.168.1.33 to 192.168.1.65. This configuration leaves 30 IP addresses (excluding the P-330W itself) in the lower range for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

4.3.3 System DNS Servers

Refer to the *IP Address and Subnet Mask* section in the **Setup Wizard** chapter.

4.3.4 LAN TCP/IP

The P-330W has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

4.3.5 Factory LAN Defaults

The LAN parameters of the P-330W are preset in the factory with the following values:

- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 33 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), read the embedded web configurator help regarding what fields need to be configured.

4.3.6 IP Address and Subnet Mask

Refer to the *IP Address and Subnet Mask* section in the **Wizard Setup** chapter for this information.

4.3.7 Configuring IP

Click **LAN** to open the **IP** screen.

Figure 16 LAN IP Setup

The following table describes the labels in this screen.

Table 14 LAN IP Setup

LABEL	DESCRIPTION
IP Address	Type the IP address of your P-330W in dotted decimal notation 192.168.1.1 (factory default).
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your P-330W will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the P-330W 255.255.255.0.
DHCP	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Choose **Server** box selected unless your ISP instructs you to do otherwise. Choose **Disabled** the P-330W acting as a DHCP server. When configured as a server, the P-330W provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must be manually configured. When set as a server, fill in the following four fields.
DHCP Client Range	This field specifies the contiguous addresses in the IP address pool.
Show DHCP Client	Push this button opens a new window which will show you a list of the clients that have recieved an IP address from the internal DHCP server.
Save	Click **Apply** to save your changes back to the P-330W.
Reset	Click **Reset** to begin configuring this screen afresh.

4.4 Configuring Password

To change your P-330W's password (recommended), click the **Password** tab. The screen appears as shown. This screen allows you to change the P-330W's password.

Figure 17 Password

The following table describes the labels in this screen.

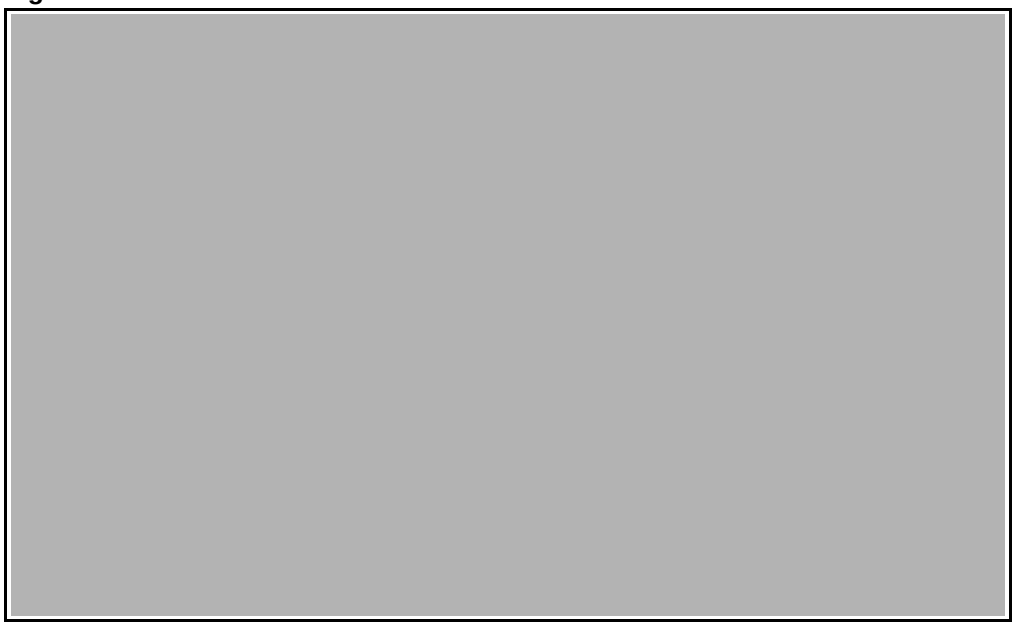
Table 15 Password

LABEL	DESCRIPTION
New Password	Type the new password in this field. The password is case sensitive and may be up to 36 characters long.
Confirmed Password	Type the new password again in this field.
Save	Click **Save** to save your changes back to the P-330W.
Reset	Click **Reset** to begin configuring this screen afresh.

4.5 Status Screen

Click **STATUS** to open the **Status** screen, which you can use to monitor your P-330W. Note that these fields are READ-ONLY and only for diagnostic purposes.

Figure 18 Status



The following table describes the labels in this screen.

Table 16 Status

LABEL	DESCRIPTION
Connection Method	This is the method you have selected for connection to the Internet. You can change it using the **Setup Wizard**.
Internet IP Address	This is the WAN port IP address.
Connection Details	This button opens a new window that provides you with more detail on the WAN connection.
LAN	
IP Address	This is the LAN port IP address.
IP Subnet Mask	This is the LAN port subnet mask.
DHCP Server	This is the LAN port DHCP role - **Server (ON)** or **Disabled**.
System	
Firmware Version	Displays the current version number of the firmware on the P-330W.
System Data	Provides a greater level of detail on your current system configuration.
Refresh Screen	Causes the P-330W to refresh the screen with the latest information.

CHAPTER 5
Wireless

This chapter discusses how to configure the Wireless screens on the P-330W.

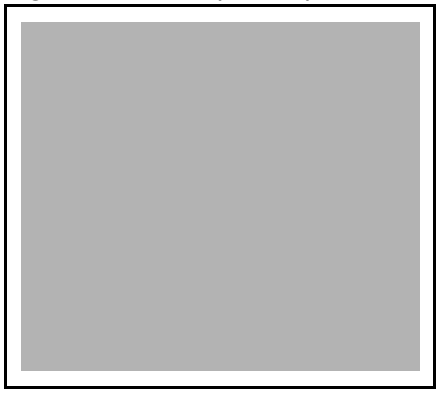
5.1 Wireless LAN Overview

This section introduces the wireless LAN(WLAN) and some basic scenarios.

5.1.1 IBSS

An Independent Basic Service Set (IBSS), also called an Ad-hoc network, is the simplest WLAN configuration. An IBSS is defined as two or more computers with wireless adapters within range of each other that from an independent (wireless) network without the need of an access point (AP).

Figure 19 IBSS (Ad-hoc) Wireless LAN

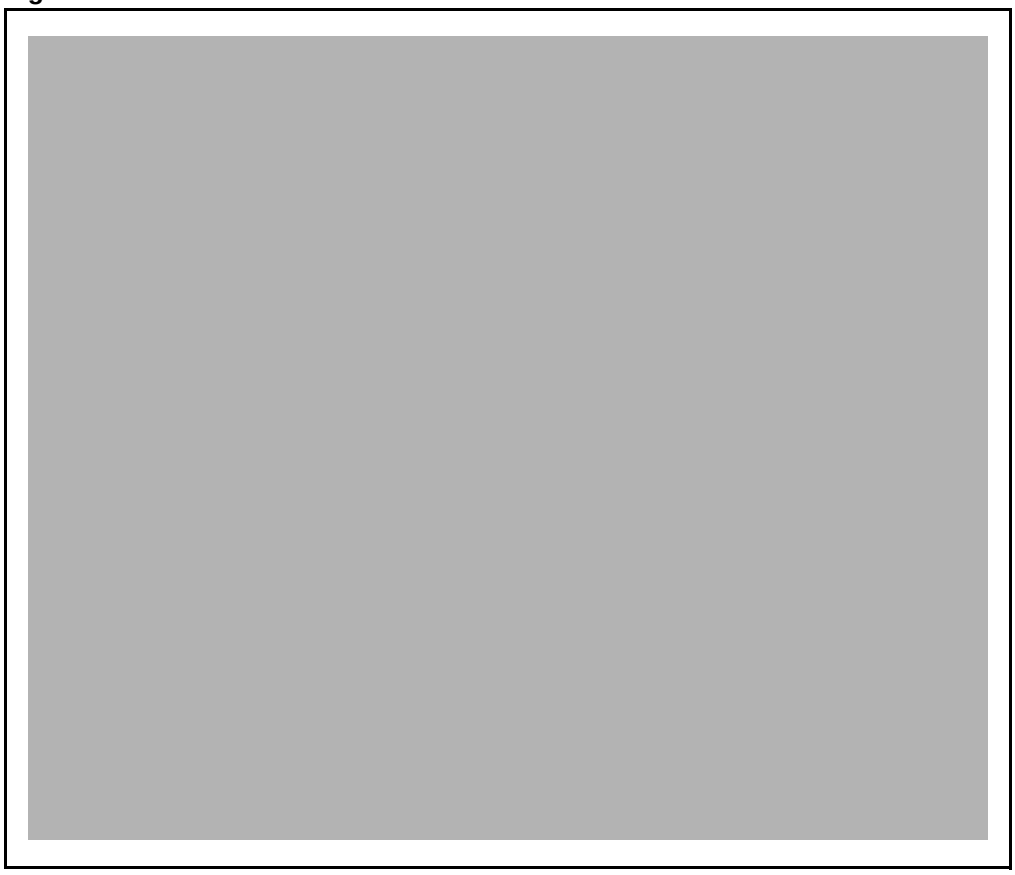


5.1.2 BSS

A Basic Service Set (BSS) exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS is enabled, wireless station A and B can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless station A and B can still access the wired network but cannot communicate with each other.

Figure 20 Basic Service set



5.1.3 ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS). An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless stations within the same ESS must have the same ESSID in order to communicate.

Figure 21 Extended Service Set

5.1.4 RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

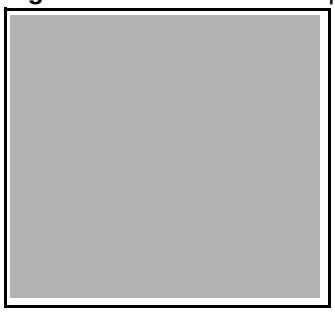
Figure 22 RTS/CTS

When station A sends data to the P-330W, it might not know that station B is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

5.2 Configuring Wireless

Click the **WIRELESS** link to open the **Wireless Options** screen.

Figure 23 The Wireless Options Screen



5.3 Basic Settings

Click **BASIC SETTINGS** to configure the basic settings of your wireless LAN.

Figure 24 Wireless: Basic Settings

The following table describes the basic wireless LAN labels in this screen.

Table 17 Wireless: Basic Settings

LABEL	DESCRIPTION
Disable Access Point	Select this check box to disable the wireless LAN capabilities of your P-330W.
Band	Choose the operating mode of your wireless access point. **2.4Ghz (B+G)** offers the greatest compatibility. **2.4 GHz (B)** will only allow 802.11b clients to connect to the wireless LAN. **2.4 GHz (G)** will only allow 802.11g clients to connect to the wireless LAN.
Mode	Mode allows you to change the wireless behavior of the P-330W. **AP** allows wireless clients to connect to the P-330W. **Client** mode activates the Wireless ISP mode of the router. Use this mode to connect to a WISP or metro-area wireless network.
Network Type	Used when operating in Client mode. This allows you to switch between **Infrastructure** and **Ad Hoc** networking modes.
SSID	(Service Set IDentity) The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. **Note:** If you are configuring the P-330W from a computer connected to the wireless LAN and you change the P-330W's SSID or WEP settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the P-330W's new settings.
Channel Number	To manually set the P-330W to use a channel, select a channel from the drop-down list box.
Associated Clients	Click **Show Active Clients** to be shown a list of wireless clients currently connected to the Wireless LAN
Save	Click **Save** to save your changes back to the P-330W.
Reset	Click **Reset** to reload the previous configuration for this screen.

5.4 Wireless Advanced Settings

Click **ADVANCED SETTINGS** to configure the advanced settings of your wireless LAN.

5.4.1 Authentication

Three different methods can be used to authenticate wireless stations to the network: **Open System**, **Shared Key**, and **Auto**. The following figure illustrates the steps involved.

Figure 25 WEP Authentication Steps

Open system authentication involves an unencrypted two-message procedure. A wireless station sends an open system authentication request to the AP, which will then automatically accept and connect the wireless station to the network. In effect, open system is not authentication at all as any station can gain access to the network.

Shared key authentication involves a four-message procedure. A wireless station sends a shared key authentication request to the AP, which will then reply with a challenge text message. The wireless station must then use the AP's default WEP key to encrypt the challenge text and return it to the AP, which attempts to decrypt the message using the AP's default WEP key. If the decrypted message matches the challenge text, the wireless station is authenticated.

When your P-330W's authentication method is set to open system, it will only accept open system authentication requests. The same is true for shared key authentication. However, when it is set to auto authentication, the P-330W will accept either type of authentication request and the P-330W will fall back to use open authentication if the shared key does not match.

5.4.2 Preamble Type

A preamble is used to synchronize the transmission timing in your wireless network. There are two preamble modes: **Long** and **Short**.

Short preamble takes less time to process and minimizes overhead, so it should be used in a good wireless network environment when all wireless clients support it.

Select **Long** if you have a 'noisy' network or are unsure of what preamble mode your wireless clients support as all IEEE 802.11b compliant wireless adapters must support long preamble. However, not all wireless adapters support short preamble. Use long preamble if you are unsure what preamble mode the wireless adapters support, to ensure interpretability between the P-330W and the wireless stations and to provide more reliable communication in 'noisy' networks..

Figure 26 Wireless: Advanced Settings

The following table describes the advanced wireless LAN labels in this screen.

Table 18 Wireless: Advanced Settings

LABEL	DESCRIPTION
Authentication Type	Select Auto, Open System or Shared Key from the menu..
Preamble Type	Select a preamble type from the drop-down list menu. Choices are Long or Short. The default setting is Long.

Table 18 Wireless: Advanced Settings

LABEL	DESCRIPTION
Broadcast SSID	Select this to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through passive scanning using a site survey tool.
IAPP	Used in a multiple AP environment where 802.1x is used for authentication.
Save	Click **Save** to save your changes back to the P-330W.
Reset	Click **Reset** to reload the previous configuration for this screen.

5.5 Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless stations, access points and the wired network.

The figure below shows the possible wireless security levels. EAP (Extensible Authentication Protocol) is used for authentication and utilizes dynamic WEP key exchange. It requires interaction with a RADIUS (Remote Authentication Dial-In User Service) server either on the WAN or your LAN to provide authentication service for wireless stations.

Figure 27 P-330W Wireless Security Levels

If you do not enable any wireless security on your P-330W, your network is accessible to any wireless networking device that is within range.

Select **NONE** for **Encryption** to allow wireless stations to communicate with the access points without any data encryption.

Figure 28 Wireless Security Setup: No Security

The following table describes the labels in this screen.

Table 19 Wireless Security Setup: No Security

LABEL	DESCRIPTION
Encryption	Choose **None** from the drop-down list box.
Use 802.1x Authentication	Mark this check box to enable 802.1x security using an external RADIUS server. Data will not be encrypted, however wireless clients will be required to authenticate before they are allowed to pass traffic to the network. Both the client and the RADIUS server will need to support the same EAP protocols.
Save	Click **Save** to save your changes back to the P-330W.
Reset	Click **Reset** to reload the previous configuration for this screen.

5.6 Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. You enter manual keys by first selecting **64-bit WEP** or **128-bit WEP** from the **WEP Encryption** field and then typing the keys (in ASCII or hexadecimal format) in the key text boxes. MAC address filters are not dependent on how you configure these security features.

Table 20 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	
Open	None	No	Disabled
Open	WEP	No	Enable with 802.1x
		Yes	Disabled
Shared	WEP	No	Enable with 802.1x
		Yes	Disable
WPA	TKIP	No	Enable
WPA-PSK	TKIP	Yes	Disabled
WPA2	AES	No	Enable
WPA2-PSK	AES	Yes	Disabled
WPA2-Mixed	AES & TKIP	No	Enable
WPA2-Mixed PSK	AES & TKIP	Yes	Disabled

5.6.1 WEP Overview

WEP (Wired Equivalent Privacy) as specified in the IEEE 802.11 standard provides methods for both data encryption and wireless station authentication.

5.6.2 Data Encryption

WEP provides a mechanism for encrypting data using encryption keys. Both the AP and the wireless stations must use the same WEP key to encrypt and decrypt data. Your P-330W allows you to configure up to four 64-bit or 128-bit WEP keys, but only one key can be enabled at any one time.

5.6.3 Configuring WEP Encryption

In order to configure and enable WEP encryption; click the **SECURITY** link under **WIRELESS** to display the **Wireless Security** screen. Select **Static WEP** from the **Encryption** list.

Figure 29 Wireless Security Setup: WEP Encryption

The following table describes the wireless LAN security labels in this screen

Table 21 Wireless Security Setup: Static WEP Encryption

LABEL	DESCRIPTION
Encryption	Choose **WEP** from the drop-down list box.
Set WEP Key	Click this to configure WEP without 802.1x.
Use 802.1x Authentication	Mark the check box here to use 802.1x authentication.
WEP Encryption	Select **64-bit WEP** or **128-bit WEP**. Used only when using 802.1x authentication.
Authentication RADIUS Server	
Port	The port number on the RADIUS server.
IP Address	Enter the IP address of the RADIUS server.
Password	Enter the password (shared secret) for the RADIUS server.
Save	Click **Save** to save your changes back to the P-330W.
Reset	Click **Reset** to reload the previous configuration for this screen.

Click SET WEP KEY to configure WEP encryption.

Figure 30 Wireless Security Setup: WEP Encryption

The following table describes the wireless LAN security labels in this screen

Table 22 Wireless Security Setup: WEP Encryption

	DESCRIPTION
Key Length	Select **64-bit WEP** or **128-bit WEP**.
Key Format	ASCII: Select this option in order to enter ASCII characters as WEP key. Hex: Select this option in order to enter hexadecimal characters as a WEP key.
Default Tx Key	You must configure at least one key, only one key can be activated at any one time. The default key is key 1.
Encryption Key 1 to 4	The WEP keys are used to encrypt data. Both the P-330W and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").
Passphrase	Enter a Passphrase (up to 32 printable characters) and clicking **Generate WEP KEY**. The P-330W automatically generates a WEP key.
Save	Click **Save** to save your changes back to the P-330W.
Close	Click **Close** to close this window.
Reset	Click **Reset** to reload the previous configuration for this screen.

5.6.4 Introduction to WPA

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security specification draft. Key differences between WPA and WEP are user authentication and improved data encryption.

5.6.4.1 User Authentication

WPA applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. See later in this chapter and the appendices for more information on IEEE 802.1x, RADIUS and EAP. Your wireless client will need to be able to support 802.1x authentication to use RADIUS authentication.

Therefore, if you don't have an external RADIUS server you should use WPA-PSK (WPA - Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a client will be granted access to a WLAN.

5.6.4.2 Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x.

Temporal Key Integrity Protocol (TKIP) uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

TKIP regularly changes and rotates the encryption keys so that the same encryption key is never used twice. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), TKIP makes it much more difficult to decode data on a Wi-Fi network than WEP, making it difficult for an intruder to break into the network.

The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs an easier-to-use, consistent, single, alphanumeric password.

5.6.4.3 WPA-PSK Application Example

A WPA-PSK application looks as follows.

1. First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters (including spaces and symbols).
2. The AP checks each client's password and (only) allows it to join the network if it matches its password.
3. The AP derives and distributes keys to the wireless clients.
4. The AP and wireless clients use the TKIP encryption process to encrypt data exchanged between them.

Figure 31 WPA - PSK Authentication

5.6.5 Introduction to WPA2

WPA2 is based on the same 802.11i spec as WPA. The primary difference between WPA and WPA2 is that WPA2 uses AES encryption in places of TKIP. Like WPA, WPA2 can function either using a pre-shared key or by using a RADIUS server to perform authentication. WPA2 also offers a mixed mode which allows WPA clients to authenticate and use TKIP encryption while still allowing WPA2 clients to use AES. Configuration of WPA2 is the same as WPA.

5.6.6 Configuring WPA-PSK Authentication

In order to configure and enable WPA-PSK encryption; click the **SECURITY** link under **WIRELESS** to display the **Wireless Security** screen. Select **WPA (TKIP)** from the **Encryption** list. Select **PERSONAL** under **WPA Encryption Mode**.

Figure 32 Wireless Security Setup: WPA-PSK

The following table describes the labels in this screen.

Table 23 Wireless Security Setup: WPA-PSK

LABEL	DESCRIPTION
Encryption	Choose **WPA (TKIP)** from the drop-down list box for TKIP encryption. Choose **WPA2 (AES)** from the drop-down list box to use WPA2's AES encryption. Choose **WPA2 Mixed** from the drop-down list box to allow both TKIP or AES encryption.
WPA Authentication Mode	Choose **Personal** to enable PSK mode.
WPA Format	Choose whether to enter the PSK by either **Passphras**e or **Hex** key.
Pre-Shared Key	The encryption mechanisms used for **WPA** and **WPA-PSK** are the same. The only difference between the two is that **WPA-PSK** uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hex characters.
Group Key Life TIme	The **Group Key Life Time** is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis.
Save	Click **Save** to save your changes back to the P-330W.
Reset	Click **Reset** to reload the previous configuration for this screen.

5.6.7 Introduction to RADIUS

RADIUS is based on a client-sever model that supports authentication and accounting, where access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks among others:

- Authentication

  Determines the identity of the users.

- Accounting

  Keeps track of the client's network activity.

RADIUS user is a simple package exchange in which your P-330W acts as a message relay between the wireless station and the network RADIUS server.

5.6.7.1 Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.

- Access-Reject

  Sent by a RADIUS server rejecting access.

- Access-Accept

  Sent by a RADIUS server allowing access.

5.6.7.2 Access-Challenge

Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

5.6.7.3 Accounting-Request

Sent by the access point requesting accounting.

5.6.7.4 Accounting-Response

Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the wired network from unauthorized access.

5.6.7.5 EAP Authentication Overview

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, the access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server or the AP. The P-330W supports EAP-TLS, EAP-TTLS and PEAP with RADIUS. Refer to the *Types of EAP Authentication* appendix for descriptions on the four common types.

Your P-330W supports EAP-MD5 (Message-Digest Algorithm 5) with RADIUS.

The following figure shows an overview of authentication when you specify a RADIUS server on your access point.

Figure 33 EAP Authentication

The details below provide a general description of how IEEE 802.1x EAP authentication works. For an example list of EAP-MD5 authentication steps, see the IEEE 802.1x appendix.

1. The wireless station sends a "start" message to the P-330W.
2. The P-330W sends a "request identity" message to the wireless station for identity information.
3. The wireless station replies with identity information, including username and password.
4. The RADIUS server checks the user information against its user profile database and determines whether or not to authenticate the wireless station.

5.6.7.6 WPA with RADIUS Application Example

You need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.

2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.

3 The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 34 WPA with RADIUS Application Example

5.6.8 Configuring WPA Authentication

In order to configure and enable WPA encryption; click the **SECURITY** link under **WIRELESS** to display the **Wireless Security** screen. Select the mode **(WPA, WPA2, WPA2 Mixed)** from the **Encryption** list. Select **ENTERPRISE** under **WPA Encryption Mode**.

Figure 35 Wireless Security Setup: WPA With RADIUS

The following table describes the labels in this screen.

Table 24 Wireless Security Setup: WPA

LABEL	DESCRIPTION
Encryption	Choose **WPA (TKIP)** from the drop-down list box for TKIP encryption. Choose **WPA2 (AES)** from the drop-down list box to use WPA2's AES encryption. Choose **WPA2 Mixed** from the drop-down list box to allow both TKIP or AES encryption.
WPA Group Key Update Timer	The **WPA Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK** key management) or **RADIUS** server (if using WPA key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **WPA Group Key Update Timer** is also supported in **WPA-PSK** mode. The P-330W default is **1800** seconds (30 minutes).
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port	Enter the port number of the external authentication server. The default port number is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.

Table 24 Wireless Security Setup: WPA

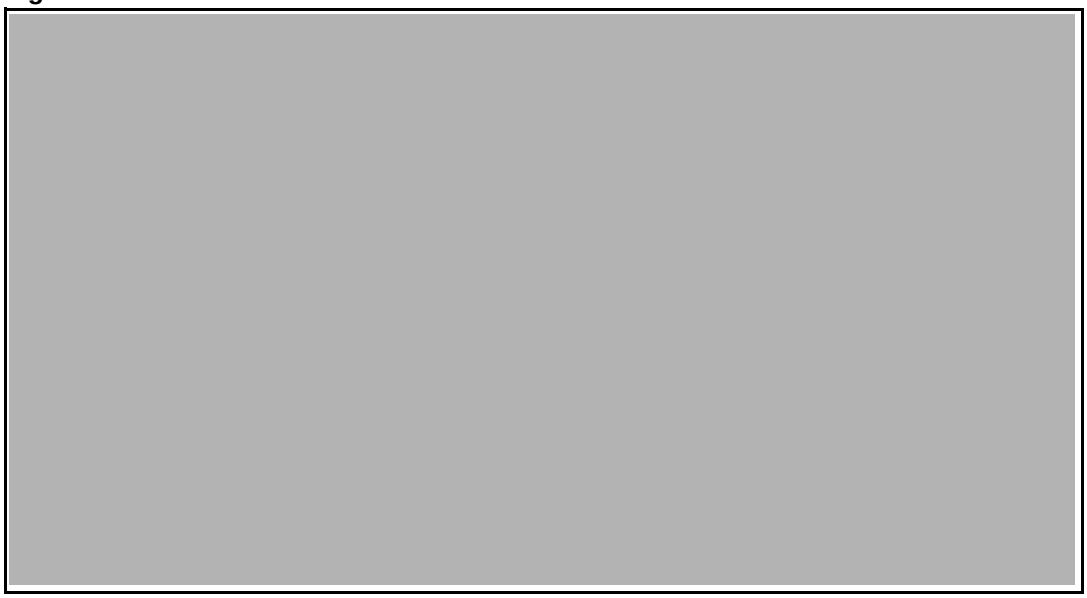
LABEL	DESCRIPTION
Password	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the P-330W. The key must be the same on the external authentication server and your P-330W. The key is not sent over the network.
Save	Click **Save** to save your changes back to the P-330W.
Reset	Click **Reset** to reload the previous configuration for this screen.

5.7 Wireless Trusted Stations

The Trusted Stations screen allows you to configure the P-330W to give exclusive access to up to 20 devices. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

To change your P-330W's Trusted Stations settings, click the **WIRELESS** link, then the **Trusted Stations** link. The screen appears as shown.

Figure 36 Wireless: Trusted Stations MAC Address Filter



The following table describes the labels in this menu.

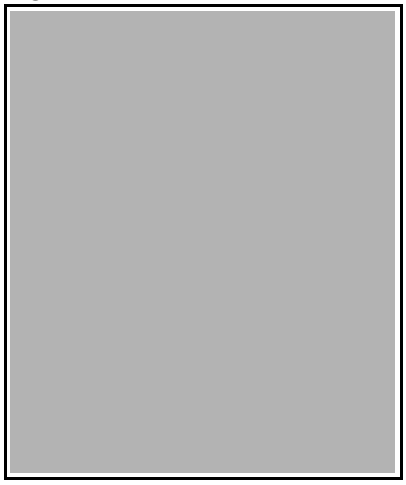
Table 25 Wireless: Trusted Stations MAC Address Filter

LABEL	DESCRIPTION
Wireless Access Control Mode	Select **Allow Listed** from the drop down list box to enable MAC address filtering.
MAC Address	Enter the MAC addresses of the wireless station that are allowed or denied access to the P-330W in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Description	Enter in a descriptive name so you know which device the MAC address is associated with.
Save	Click **Save** to save your changes back to the P-330W.
Reset	Click **Reset** to reload the previous configuration for this screen.
Current Access Control List	
Delete Selected	Click this button to delete selected clients from the trusted station list.
Delete All	Click this button to delete all clients from the trusted station list.

CHAPTER 6
Advanced Options

This chapter covers the options available under the **ADVANCED** section of the menu.

Figure 37 The Advanced Menu Options

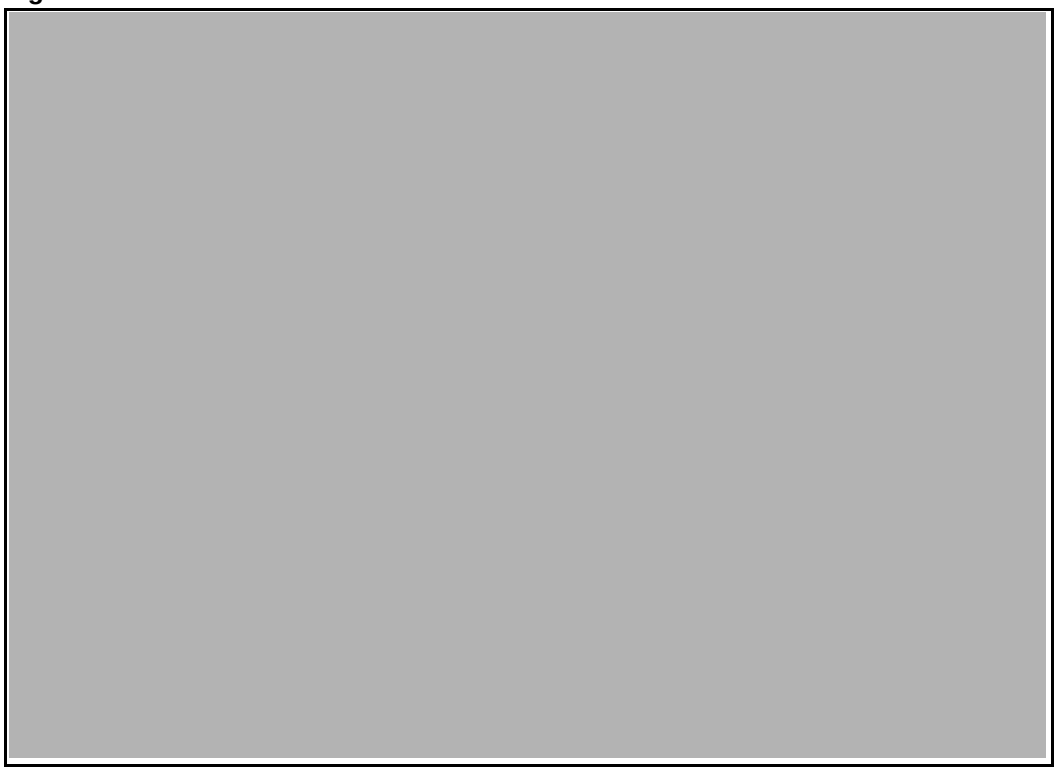


6.1 Access Control

This screen allows you to block access to specified Internet services based on port number used. This can be used restrict Internet access to only certain applications or to block applications you feel may be harmful.

To change your P-330W's Access Controls, click **ADVANCED**, then the **Access Control** link. The screen appears as shown.

Figure 38 Advanced: Access Control



The following table describes the labels in this screen.

Table 26 Advanced: Access Control

LABEL	DESCRIPTION
Enable Access Control	Check this box to enable Access Controls.
Select Services to Block	The P-330W comes preconfigured with settings for many common services. You can choose one to activate from the pull down menu.
Port Range	Enter in a range of ports to block.
Protocol	Choose to block either TCP, UDP, or Both.
Description	Give the rule you have created an easy to identify name.
Save	Click **Save** to save your changes back to the P-330W.
Reset	Click **Reset** to begin configuring this screen afresh.

6.2 Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with either www.dyndns.org or www.tzo.com. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

6.3 Configuring Dynamic DNS

To change your P-330W's DDNS, click **ADVANCED** then the **Dynamic DNS** link. The screen appears as shown.

Figure 39 Advanced: Dynamic DNS

The following table describes the labels in this screen.

Table 27 Advanced: Dynamic DNS

LABEL	DESCRIPTION
Enable DDNS	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Domain Name	Enter the host names in the field provided.
User Name	Enter your user name.
Password	Enter the password assigned to you.
Result	Tells you the current result from trying to register your IP address with the DDNS provider.

Table 27 Advanced: Dynamic DNS

LABEL	DESCRIPTION
Save	Click **Save** to save your changes back to the P-330W.
Reset	Click **Reset** to begin configuring this screen afresh.

6.4 DMZ

If the DMZ Host Function is enabled, it means that you set up DMZ host at a particular computer to be exposed to the Internet so that some applications/software, especially Internet / online game can have two-way connections. A device acting as DMZ is not protected by the P-330W's firewall.

To enable DMZ, click **ADVANCED** then the **DMZ** link. The screen appears as shown.

Figure 40 Advanced: DMZ

The following table describes the labels in this screen.

Table 28 Advanced: DMZ

LABEL	DESCRIPTION
Enable DMZ	Select this check box to enable DMZ.
Host IP Address	Enter the IP address of the device you which to be accessible from the Internet.
Save	Click **Save** to save your changes back to the P-330W.
Reset	Click **Reset** to begin configuring this screen afresh.

6.5 Virtual Servers (Port Forwarding)

The Virtual Server function is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. .

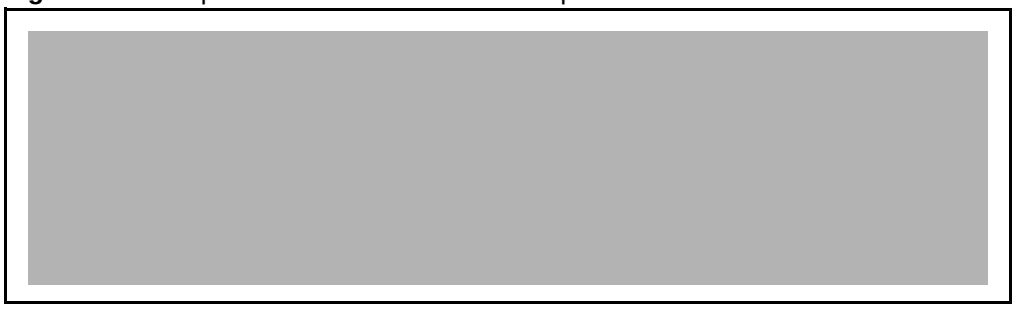
Table 29 Services and Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

6.5.0.1 Configuring Servers Behind SUA (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (A in the example), port 80 to another (B in the example) and assign a default server IP address of 192.168.1.35 to a third (C in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet

Figure 41 Multiple Servers Behind NAT Example



6.5.1 Configuring Virtual Servers

To configure Virtual Server, click **ADVANCED** then the **VIRTUAL SERVERS** link. The screen appears as shown.

Figure 42 Advanced: Virtual Servers

The following table describes the labels in this screen.

Table 30 Advanced: Virtual Servers

LABEL	DESCRIPTION
Enable Virtual Servers	Put a check in the box to enable Virtual Servers
Servers	By selection an option in the pull down menu, the P-330W will automatically populate the settings for the corresponding service.

Table 30 Advanced: Virtual Servers

LABEL	DESCRIPTION
Local IP Address	Enter the inside IP address of the server here.
Protocol	You can select to forward TCP, UDP, or both type of traffic.
Name	Enter a name to identify this port-forwarding rule.
Port Range	Enter a port number here. To forward only one port, enter it again in the **End Port** field. To specify a range of ports, enter the last port to be forwarded in the **End Port** field.
Description	Enter in a description for this Virtual Server.
Save	Click **Save** to save your changes back to the P-330W.
Reset	Click **Reset** to begin configuring this screen afresh.

6.6 ALG

ALG stands for Application Level Gateway. ALG's are used to help applications to navigate through a NAT and properly send/receive information over the Internet. You P-330W comes with several preconfigured rules for popular applications whose use will be enhanced though use of an ALG.

To change your P-330W's ALG settings, click **ADVANCED** and the **ALG** link. The screen appears as shown.

Figure 43 Advanced: ALG

The following table describes the labels in this screen.

Table 31 Advanced: ALG

LABEL	DESCRIPTION
Enable	Put a check in this box next to the ALG rule you want to activate.
Save	Click **Save** to save your changes back to the P-330W.
Reset	Click **Reset** to begin configuring this screen afresh.

6.7 WAN Port

To change your P-330W's WAN ISP settings, click **ADVANCED**, then the **WAN** link. The screen differs by the encapsulation.

6.7.1 Static IP Encapsulation

The screen shown next is for **Static IP** encapsulation.

Figure 44 Advanced: WAN Static IP Encapsulation

The following table describes the labels in this screen.

Table 32 Advanced: WAN Static IP Encapsulation

LABEL	DESCRIPTION
WAN Access Type	You must choose the Static IP option when the WAN port is used as a regular Ethernet with a fixed IP address.
IP Address	Enter your WAN IP address in this field**.**
My WAN IP Subnet Mask	Type your network's IP subnet Mask.
DNS 1 - 3	Enter in your ISP's DNS server IP address here. You must enter in 1.
Clone MAC Address	Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in this Clone MAC address in this section to replace the WAN MAC address with the MAC address of that PC.
Enable UPnP	UPnP (Universal Plug and Play) allows automatic discovery and configuration of the Wireless Router. UPnP is by supported by Windows ME, XP, or later. Put a check in this box to allow the router configuration to be changed by UPnP devices.
IPSec Passthrough	Put a check in this box to enable computers on your LAN to make IPSec VPN connections to servers on the Internet.
PPTP Passthrough	Put a check in this box to enable computers on your LAN to make PPTP VPN connections to servers on the Internet.
L2TP Passthrough	Put a check in this box to enable computers on your LAN to make L2TP VPN connections to servers on the Internet.
Save	Click **Save** to save your changes back to the P-330W.
Reset	Click **Reset** to begin configuring this screen afresh.

6.7.2 DHCP IP Encapsulation

The screen shown next is for **DHCP IP** encapsulation.

Figure 45 Advanced: WAN DHCP IP Encapsulation

The following table describes the labels in this screen.

Table 33 Advanced: WAN DHCP IP Encapsulation

LABEL	DESCRIPTION
WAN Access Type	You must choose the DHCP Client option when the WAN port is used as a regular Ethernet using DHCP to be assigned an IP address.
Attain DNS Automatically	Select this if your ISP assigns you a DNS server at the same time it assigns you an IP Address.
Set DNS Manually	Use this if your ISP does not assign a DNSP server when it assigns you an IP address.
DNS 1 - 3	Enter in your ISP's DNS server IP address here. You must enter in 1.
Clone MAC Address	Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in this Clone MAC address in this section to replace the WAN MAC address with the MAC address of that PC.
Enable UPnP	UPnP (Universal Plug and Play) allows automatic discovery and configuration of the Wireless Router. UPnP is by supported by Windows ME, XP, or later. Put a check in this box to allow the router configuration to be changed by UPnP devices.
IPSec Passthrough	Put a check in this box to enable computers on your LAN to make IPSec VPN connections to servers on the Internet.
PPTP Passthrough	Put a check in this box to enable computers on your LAN to make PPTP VPN connections to servers on the Internet.
L2TP Passthrough	Put a check in this box to enable computers on your LAN to make L2TP VPN connections to servers on the Internet.

Table 33 Advanced: WAN DHCP IP Encapsulation

LABEL	DESCRIPTION
Save	Click **Save** to save your changes back to the P-330W.
Reset	Click **Reset** to begin configuring this screen afresh.

6.7.3 PPPoE Encapsulation

The P-330W supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPP over Ethernet** option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example Radius). PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

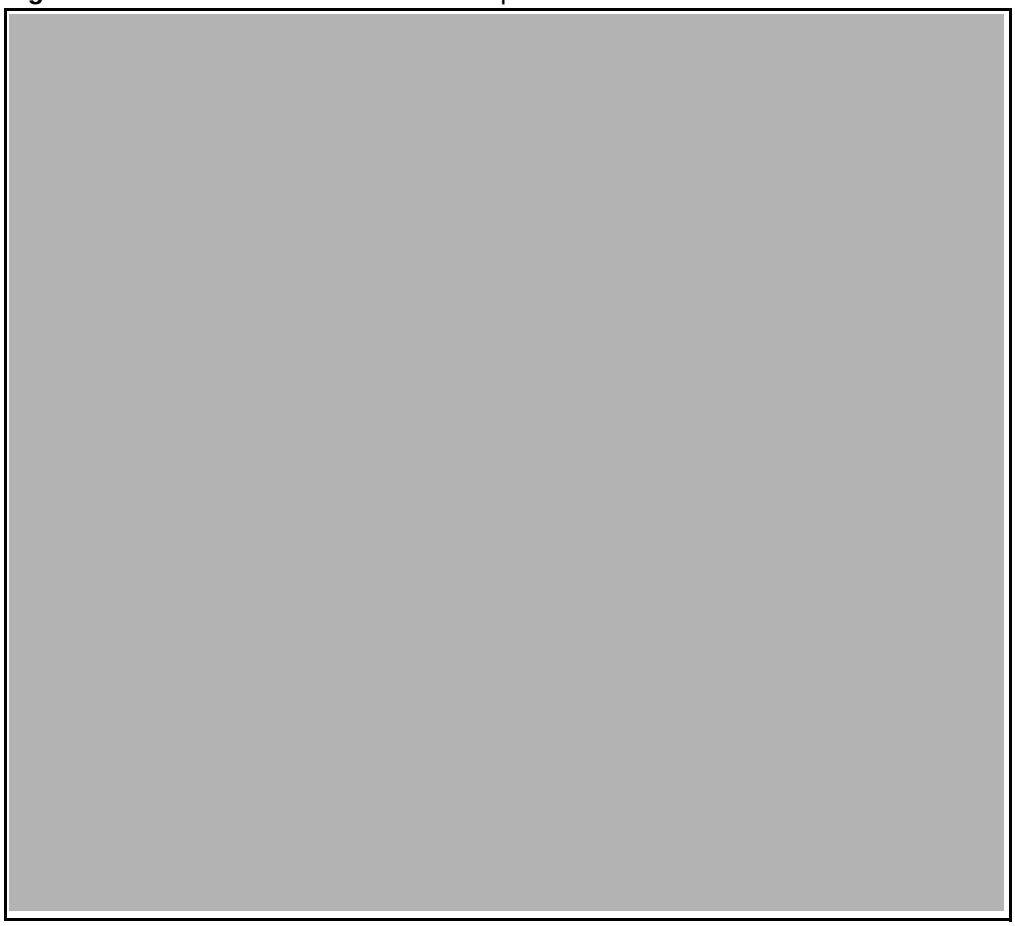
One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the P-330W (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the P-330W does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

The screen shown next is for **PPPoE** encapsulation.

Figure 46 Advanced: WAN PPPoE Encapsulation



The following table describes the labels in this screen.

Table 34 PPPoE Encapsulation

LABEL	DESCRIPTION
WAN Access Type	You must choose the PPPoE option when the WAN port is used with PPPoE.
User Name	Type the User Name given to you by your ISP.
Password	Type the password associated with the User Name above.
Connection Type	Select **Continuous** if you do not want the connection to time out. Select **Connect On Demand** if you want to only connect when you are sending data. Select **Manual** if you do not want manually log the P-330W in via the GUI.
Idle Time	The amount of time before the PPPoE session times out and drops connection.
MTU Size	Enter in the maximum MTU (packet size) here.
Attain DNS Automatically	Select this if your ISP assigns you a DNS server at the same time it assigns you an IP Address.
Set DNS Manually	Use this if your ISP does not assign a DNSP server when it assigns you an IP address.
DNS 1 - 3	Enter in your ISP's DNS server IP address here. You must enter in 1.

Table 34 PPPoE Encapsulation

LABEL	DESCRIPTION
Clone MAC Address	Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in this Clone MAC address in this section to replace the WAN MAC address with the MAC address of that PC.
Enable UPnP	UPnP (Universal Plug and Play) allows automatic discovery and configuration of the Wireless Router. UPnP is by supported by Windows ME, XP, or later. Put a check in this box to allow the router configuration to be changed by UPnP devices.
IPSec Passthrough	Put a check in this box to enable computers on your LAN to make IPSec VPN connections to servers on the Internet.
PPTP Passthrough	Put a check in this box to enable computers on your LAN to make PPTP VPN connections to servers on the Internet.
L2TP Passthrough	Put a check in this box to enable computers on your LAN to make L2TP VPN connections to servers on the Internet.
Save	Click **Save** to save your changes back to the P-330W.
Reset	Click **Reset** to begin configuring this screen afresh.

6.7.4 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

The screen shown next is for **PPTP** encapsulation.

Figure 47 Advanced: WAN PPTP Encapsulation

The following table describes the labels in this screen.

Table 35 Advanced: WAN PPTP Encapsulation

LABEL	DESCRIPTION
WAN Access Type	You must choose the PPTP option when the WAN port is used with PPTP.
IP Address	Type the (static) IP address assigned to you by your ISP.
IP Subnet Mask	Type the subnet mask assigned to you by your ISP.
Server IP Address	Type the IP address of the PPTP server.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
MTU Size	Enter in the maximum MTU (packet size) here.
Attain DNS Automatically	Select this if your ISP assigns you a DNS server at the same time it assigns you an IP Address.
Set DNS Manually	Use this if your ISP does not assign a DNSP server when it assigns you an IP address.
DNS 1 - 3	Enter in your ISP's DNS server IP address here. You must enter in 1.

Table 35 Advanced: WAN PPTP Encapsulation

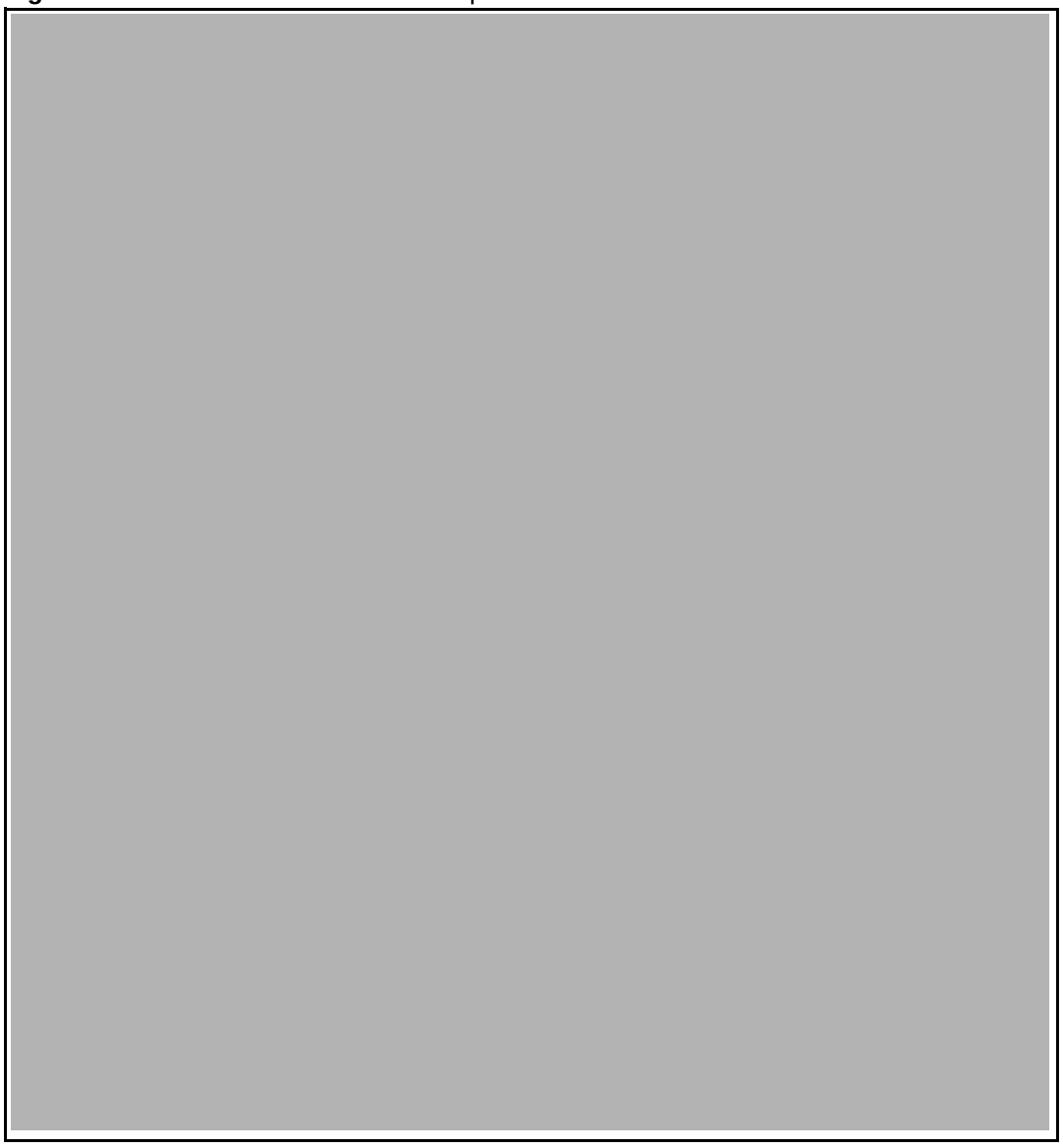
LABEL	DESCRIPTION
Clone MAC Address	Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in this Clone MAC address in this section to replace the WAN MAC address with the MAC address of that PC.
Enable UPnP	UPnP (Universal Plug and Play) allows automatic discovery and configuration of the Wireless Router. UPnP is by supported by Windows ME, XP, or later. Put a check in this box to allow the router configuration to be changed by UPnP devices.
IPSec Passthrough	Put a check in this box to enable computers on your LAN to make IPSec VPN connections to servers on the Internet.
PPTP Passthrough	Put a check in this box to enable computers on your LAN to make PPTP VPN connections to servers on the Internet.
L2TP Passthrough	Put a check in this box to enable computers on your LAN to make L2TP VPN connections to servers on the Internet.
Save	Click **Save** to save your changes back to the P-330W.
Reset	Click **Reset** to begin configuring this screen afresh.

6.7.5 L2TP Encapsulation

Layer Two Tunneling Protocol (L2TP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

The screen shown next is for **L2TP** encapsulation.

Figure 48 Advanced: WAN L2TP Encapsulation



The following table describes the labels in this screen.

Table 36 Advanced: WAN L2PTP Encapsulation

LABEL	DESCRIPTION
WAN Access Type	You must choose the L2TP option when the WAN port is used with L2TP.
Attain IP Automatically	Select this if your ISP dynamically assigns you an IP Address
Set IP Manually	Select this if your IP has assigned you a static IP address
IP Address	Type the (static) IP address assigned to you by your ISP.
IP Subnet Mask	Type the subnet mask assigned to you by your ISP.
Server IP Address	Type the IP address of the PPTP server.
User Name	Type the user name given to you by your ISP.

Table 36 Advanced: WAN L2PTP Encapsulation

LABEL	DESCRIPTION
Password	Type the password associated with the User Name above.
Idle Time	The amount of time before the PPPoE session times out and drops connection.
MTU Size	Enter in the maximum MTU (packet size) here.
Attain DNS Automatically	Select this if your ISP assigns you a DNS server at the same time it assigns you an IP Address.
Set DNS Manually	Use this if your ISP does not assign a DNSP server when it assigns you an IP address.
DNS 1 - 3	Enter in your ISP's DNS server IP address here. You must enter in 1.
Clone MAC Address	Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in this Clone MAC address in this section to replace the WAN MAC address with the MAC address of that PC.
Enable UPnP	UPnP (Universal Plug and Play) allows automatic discovery and configuration of the Wireless Router. UPnP is by supported by Windows ME, XP, or later. Put a check in this box to allow the router configuration to be changed by UPnP devices.
IPSec Passthrough	Put a check in this box to enable computers on your LAN to make IPSec VPN connections to servers on the Internet.
PPTP Passthrough	Put a check in this box to enable computers on your LAN to make PPTP VPN connections to servers on the Internet.
L2TP Passthrough	Put a check in this box to enable computers on your LAN to make L2TP VPN connections to servers on the Internet.
Save	Click **Save** to save your changes back to the P-330W.
Reset	Click **Reset** to begin configuring this screen afresh.

6.8 Ping

The Ping screen allows you to send out PING requests from your P-330W to a network address you specify and then reports back the test result. You can use this command to help diagnose network problems.

To access the Ping command, click **ADVANCED** then the **Ping** link. The screen appears as shown.

Figure 49 Advanced: Ping

The following table describes the labels in this screen.

Table 37 Advanced: Ping

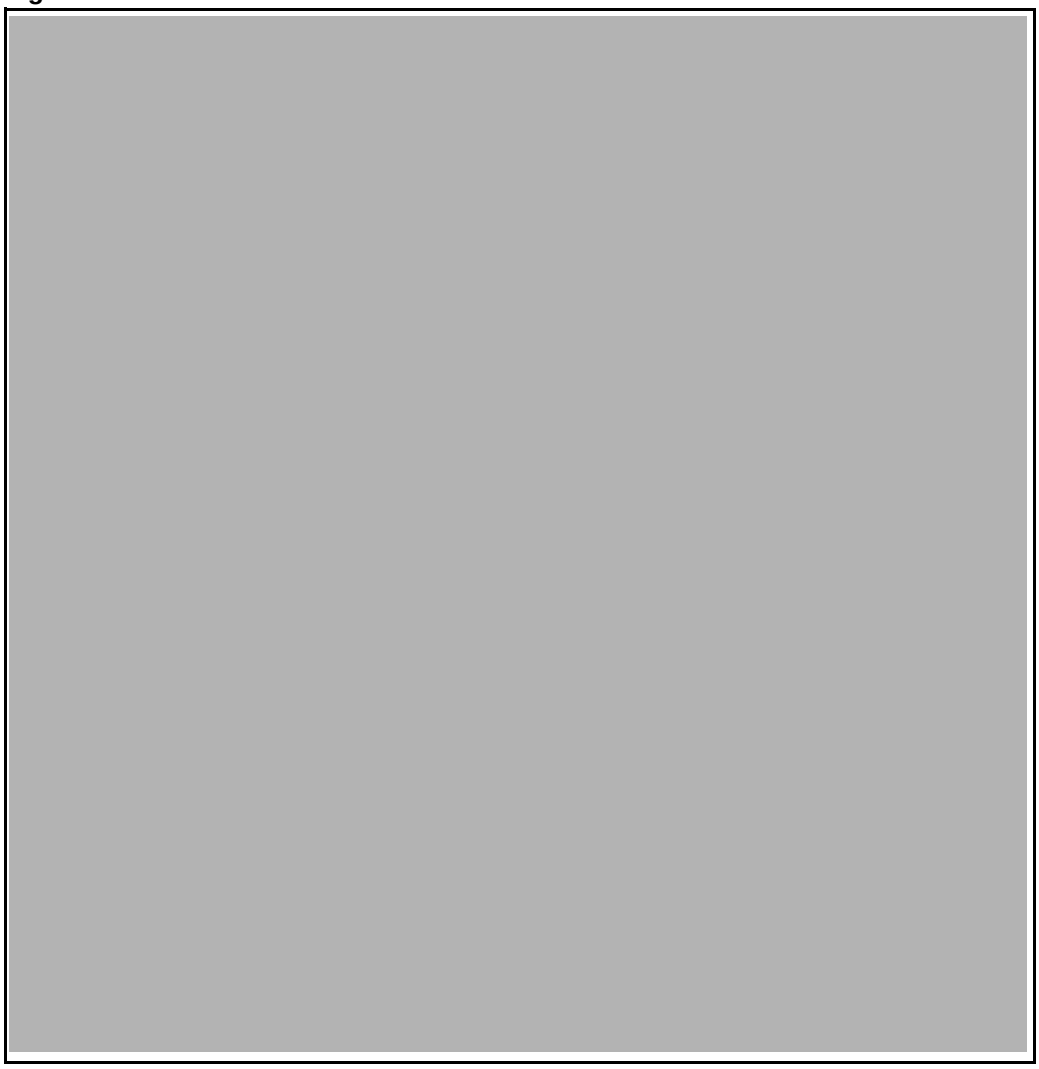
LABEL	DESCRIPTION
IP Address / Host Name	Enter in a host name or IP address that you would like to ping.
Run	Performs the Ping command.
Reset	Click **Reset** to begin configuring this screen afresh.
Response	The results of your ping request will show up here.

6.9 DoS Setting

DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. The Wireless Router incorporates protection against DoS attacks. This screen allows you to configure DoS protection.

To access the DoS settings, click **ADVANCED** then the **DoS** link. The screen appears as shown.

Figure 50 Advanced: DoS



The following table describes the labels in this screen.

Table 38 Advanced: DoS

LABEL	DESCRIPTION
Enable DoS Protection	Put a check in this box to enable DoS protection.
Select All	Puts a check next to all DoS protection services.
Clear All	Resets all check boxes to blank.
Apply Changes	Applies DoS protections.

6.10 Diagnostics

This screen allows you to perform a DNS lookup on any host name you enter. This can be used to help diagnose network problems.

To access the Diagnostic service, click **ADVANCED** then the **DIAGNOSTIC** link. The screen appears as shown.

Figure 51 Advanced: Diagnostic

The following table describes the labels in this screen.

Table 39 Advanced: Diagnostic

LABEL	DESCRIPTION
Domain Name/ URL	Enter the domain name you want to lookup.
Start Lookup	Click this button to activate the DNS lookup.

CHAPTER 7
Administrator Options

7.1 Remote Management

Remote management allows you to remotely configure your P-330W over your Internet connection. Since this is a potential security risk, this feature is turned off by default.

To access the **Remote Management** configuration screen, click **ADMINISTRATOR** then the **REMOTE MANAGEMENT** link. The screen appears as shown.

Figure 52 Administrator: Remote Management

The following table describes the labels in this screen.

Table 40 Administrator: Remote Management

LABEL	DESCRIPTION
Enable Web Server Access via WAN	Put a check in this box to allow your P-330W to be accessed over the Internet.
Port Number	Enter in the port number you want the P-330W to respond on when accessed from the Internet.
Save	Click **Save** to save your changes back to the P-330W.
Reset	Click **Reset** to begin configuring this screen afresh.

7.2 Configuration Screen

Click **Administrator**, and then the **Config File** link. The screen you are presented with is next.

Figure 53 Administrator: Configuration File

7.2.1 Backup Configuration

Backup configuration allows you to back up (save) the P-330W's current configuration to a file on your computer. Once your P-330W is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Download** to save the P-330W's current configuration to your computer.

7.2.2 Restore Configuration

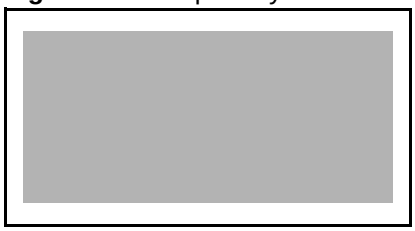
Restore configuration allows you to upload a new or previously saved configuration file from your computer to your P-330W.

Table 41 Maintenance Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Restore	Click **Restore** to begin the upload process.

The P-330W automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 54 Temporarily Disconnected



7.2.3 Back to Factory Defaults

Pressing the **Restore Defaults** button in this section clears all user-entered configuration information and returns the P-330W to its factory defaults.

You can also press the **RESET** button on the rear panel to reset the factory defaults of your P-330W. Refer to the *Introducing the Web Configurator* chapter for more information on the **RESET** button.

7.3 Logs

The Logs record various types of activity on the Wireless Router. This data is useful for troubleshooting, but enabling all logs will generate a large amount of data and adversely affect performance.

To access the **Logs** configuration screen, click **ADMINISTRATOR** then the **LOGS** link. The screen appears as shown.

Figure 55 Administrator: Logs

The following table describes the labels in this screen.

Table 42 Administrator: Remote Management

LABEL	DESCRIPTION
Enable Log	Activates the logging function.
System All	Activates all logging functions.
Wireless Only	Only logs related to the wireless LAN will be recorded.
DoS Only	Only logs related to the DoS protection will be recorded.
Apply	Activate the logging feature.
Refresh	Refreshes the current display to show the latest log activity.
Clear	Deletes the logs.

7.4 IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Router. Here you can restrict local LAN clients to access Internet application/services by IP Address. Use of such filters can be helpful in securing or restricting your local network.

To access the **IP Filtering** configuration screen, click **ADMINISTRATOR** then the **IP FILTERING** link. The screen appears as shown.

Figure 56 Administrator: IP Filtering

The following table describes the labels in this screen.

Table 43 Administrator: IP Filtering

LABEL	DESCRIPTION
Enable IP Filtering	Enables IP Filtering.
Local IP Address	Enter the IP address of the local device whose access you want to restrict.
Description	Enter in a descriptive description for this rule.
Save	Click **Save** to save your changes back to the P-330W.
Reset	Click **Reset** to begin configuring this screen afresh.

7.5 MAC Filtering

This screen is used to restrict devices on your local network from being able to access the Internet. You do this by entering the MAC address of any device you want to restrict.

To access the **MAC Filtering** configuration screen, click **ADMINISTRATOR** then the **MAC FILTERING** link. The screen appears as shown.

Figure 57 Administrator: MAC Filtering

The following table describes the labels in this screen.

Table 44 Administrator: MAC Filtering

LABEL	DESCRIPTION
Enable MAC Filtering	Enables MAC Filtering.
MAC Address	Enter the MAC address of the local device whose access you want to restrict.
Description	Enter in a descriptive description for this rule.
Save	Click **Save** to save your changes back to the P-330W.
Reset	Click **Reset** to begin configuring this screen afresh.

7.6 URL Filtering

This screen is used to restrict devices on your local network from being able to access the Internet. You can enter in a list of Internet URL's that you wish to restrict access to.

To access the **URL Filtering** configuration screen, click **ADMINISTRATOR** then the **URL FILTERING** link. The screen appears as shown.

Figure 58 Administrator: URL Filtering

The following table describes the labels in this screen.

Table 45 Administrator: URL Filtering

LABEL	DESCRIPTION
Enable URL Filtering	Enables URL Filtering.
URL Address	Enter the URL address of the Internet site you want to restrict.
Apply Changes	Click **Apply Changes** to save your changes back to the P-330W.
Reset	Click **Reset** to begin configuring this screen afresh.

7.7 Statistics

The statistics screen provides you with information on each interface on your P-330W. This includes the WAN, LAN, and wireless network connections. This page will show you how many packets of data have been sent and received.

7.8 Time Zone Setting

To change your P-330W's time and date, click **ADMINISTRATOR**, then the **Time Zone Setting** link. The screen appears as shown. Use this screen to configure the P-330W's time based on your local time zone.

Figure 59 Administrator: Time Zone Setting

The following table describes the labels in this screen.

Table 46 Administrator: Time Zone Setting

LABEL	DESCRIPTION
Current Time	This field displays the time of your P-330W. If you are not using an NTP server, you can make changes here and they will be applied when you click **Save**.
Enable NTP client update	Put a check in this box to enable the use of an external NTP server.
Time Zone Select	Choose the Time Zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
NTP Server	Enter the IP address or choose from a list of known public NTP servers. Check with your ISP/network administrator if you are unsure of this information.
Save	Click **Save** to save your changes back to the P-330W.
Reset	Click **Reset** to begin configuring this screen afresh.
Refresh	Click **Refresh** to display the current time.

7.9 Upgrade Firmware

Find firmware at www.us.zyxel.com in a file that (usually) uses the system model name with a "*.bin" extension, e.g., "P-330W.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Click **Administrator**, and then the **Upgrade Firmware** link. Follow the instructions in this screen to upload firmware to your P-330W.

Figure 60 Administrator: Upgrade Firmware

The following table describes the labels in this screen.

Table 47 Administrator: Upgrade Firmware

LABEL	DESCRIPTION
Select File	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Start Upgrade	Click **Start Upgrade** to begin the upload process. This process may take up to two minutes.

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the P-330W again.

Figure 61 Upload Warning

The P-330W automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 62 Network Temporarily Disconnected

After two minutes, log in again and check your new firmware version in the **System Status** screen.

If the upload was not successful, a warning screen will appear. Click **Return** to go back to the **F/W Upload** screen.

Appendix A PPPoE

PPPoE in Action

An ADSL modem bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your computer to an ATM PVC (Permanent Virtual Circuit) which connects to a DSL Access Concentrator where the PPP session terminates (see the next figure). One PVC can support any number of PPP sessions from your LAN. PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP.

Benefits of PPPoE

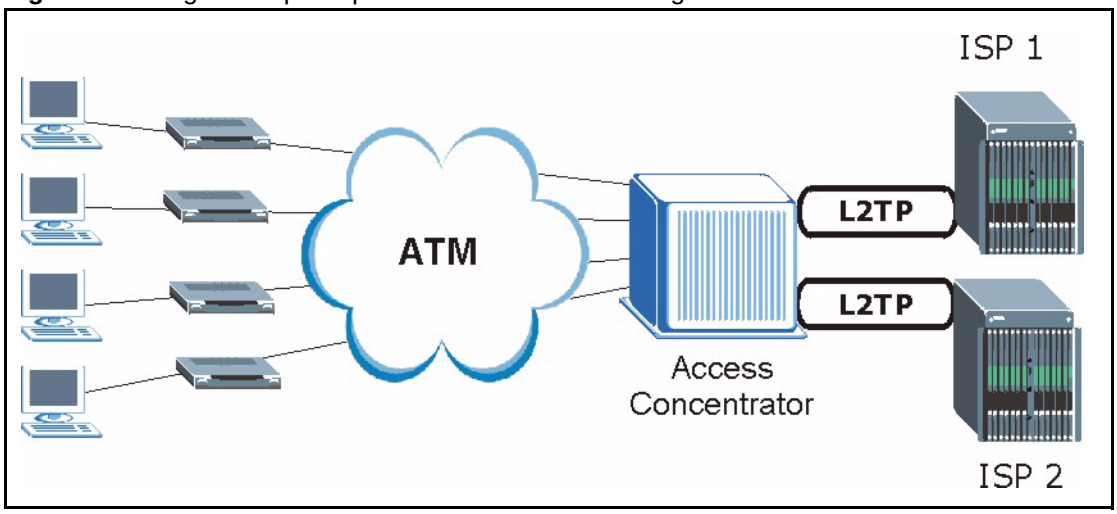
PPPoE offers the following benefits:

- It provides you with a familiar dial-up networking (DUN) user interface.
- It lessens the burden on the carriers of provisioning virtual circuits all the way to the ISP on multiple switches for thousands of users. For GSTN (PSTN and ISDN), the switching fabric is already in place.
- It allows the ISP to use the existing dial-up model to authenticate and (optionally) to provide differentiated services.

Traditional Dial-up Scenario

The following diagram depicts a typical hardware configuration where the computers use traditional dial-up networking.

Figure 63 Single-Computer per Router Hardware Configuration



How PPPoE Works

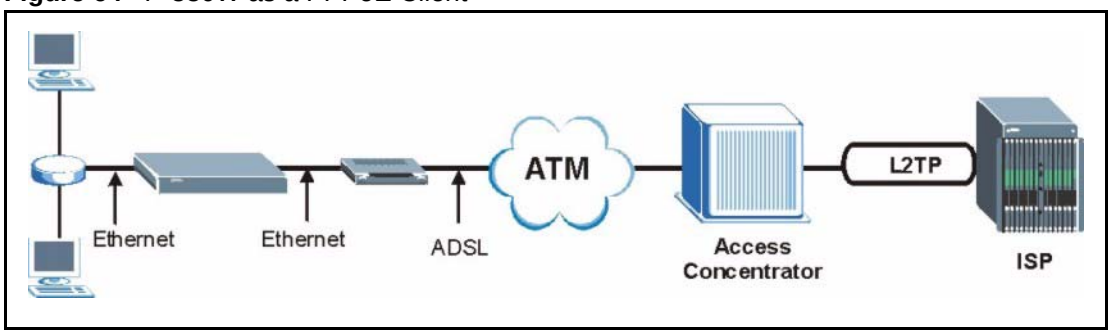
The PPPoE driver makes the Ethernet appear as a serial link to the computer and the computer runs PPP over it, while the modem bridges the Ethernet frames to the Access Concentrator (AC). Between the AC and an ISP, the AC is acting as a L2TP (Layer 2 Tunneling Protocol) LAC (L2TP Access Concentrator) and tunnels the PPP frames to the ISP. The L2TP tunnel is capable of carrying multiple PPP sessions.

With PPPoE, the VC (Virtual Circuit) is equivalent to the dial-up connection and is between the modem and the AC, as opposed to all the way to the ISP. However, the PPP negotiation is between the computer and the ISP.

P-330W as a PPPoE Client

When using the P-330W as a PPPoE client, the computers on the LAN see only Ethernet and are not aware of PPPoE. This alleviates the administrator from having to manage the PPPoE clients on the individual computers.

Figure 64 P-330W as a PPPoE Client



Appendix B PPTP

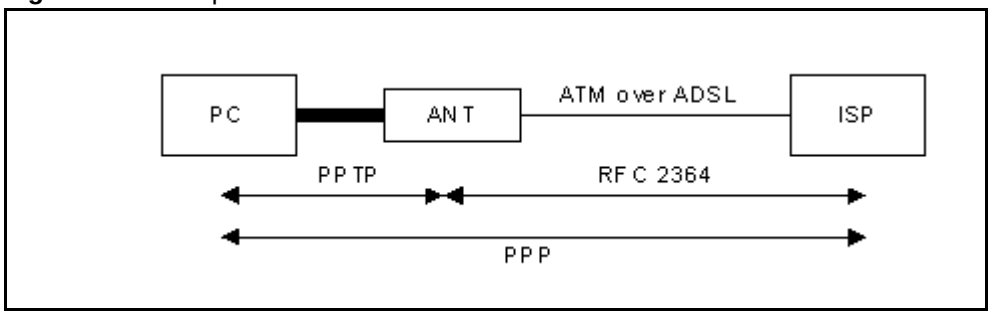
What is PPTP?

PPTP (Point-to-Point Tunneling Protocol) is a Microsoft proprietary protocol (RFC 2637 for PPTP is informational only) to tunnel PPP frames.

How can we transport PPP frames from a computer to a broadband modem over Ethernet?

A solution is to build PPTP into the ANT (ADSL Network Termination) where PPTP is used only over the short haul between the computer and the modem over Ethernet. For the rest of the connection, the PPP frames are transported with PPP over AAL5 (RFC 2364) The PPP connection, however, is still between the computer and the ISP. The various connections in this setup are depicted in the following diagram. The drawback of this solution is that it requires one separate ATM VC per destination.

Figure 65 Transport PPP frames over Ethernet



PPTP and the P-330W

When the P-330W is deployed in such a setup, it appears as a computer to the ANT.

In Windows VPN or PPTP Pass-Through feature, the PPTP tunneling is created from Windows 95, 98 and NT clients to an NT server in a remote location. The pass-through feature allows users on the network to access a different remote server using the P-330W's Internet connection. In SUA/NAT mode, the P-330W is able to pass the PPTP packets to the internal PPTP server (i.e. NT server) behind the NAT. You need to configure port forwarding for port 1723 to have the P-330W forward PPTP packets to the server. In the case above as the remote PPTP Client initializes the PPTP connection, the user must configure the PPTP clients. The P-330W initializes the PPTP connection hence; there is no need to configure the remote PPTP clients.

PPTP Protocol Overview

PPTP is very similar to L2TP, since L2TP is based on both PPTP and L2F (Cisco's Layer 2 Forwarding). Conceptually, there are three parties in PPTP, namely the PNS (PPTP Network Server), the PAC (PPTP Access Concentrator) and the PPTP user. The PNS is the box that hosts both the PPP and the PPTP stacks and forms one end of the PPTP tunnel. The PAC is the box that dials/answers the phone calls and relays the PPP frames to the PNS. The PPTP user is not necessarily a PPP client (can be a PPP server too). Both the PNS and the PAC must have IP connectivity; however, the PAC must in addition have dial-up capability. The phone call is between the user and the PAC and the PAC tunnels the PPP frames to the PNS. The PPTP user is unaware of the tunnel between the PAC and the PNS.

Figure 66 PPTP Protocol Overview

Microsoft includes PPTP as a part of the Windows OS. In Microsoft's implementation, the computer, and hence the P-330W, is the PNS that requests the PAC (the ANT) to place an outgoing call over AAL5 to an RFC 2364 server.

Control & PPP Connections

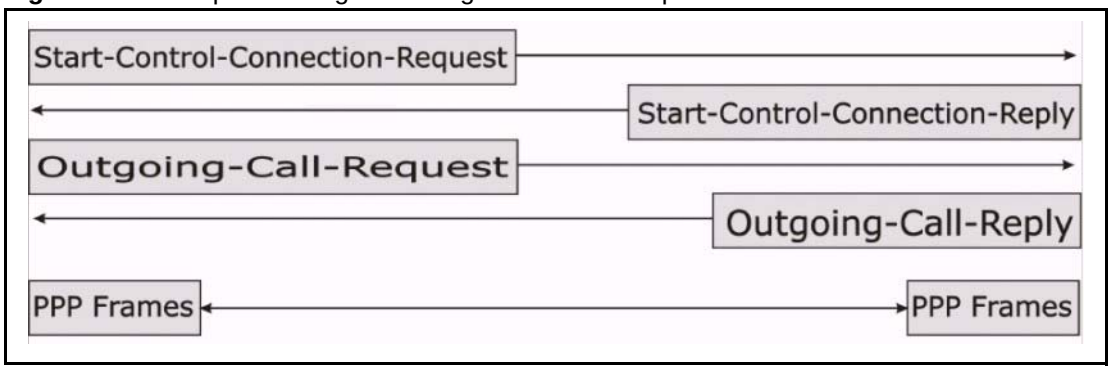
Each PPTP session has distinct control connection and PPP data connection.

Call Connection

The control connection runs over TCP. Similar to L2TP, a tunnel control connection is first established before call control messages can be exchanged. Please note that a tunnel control connection supports multiple call sessions.

The following diagram depicts the message exchange of a successful call setup between a computer and an ANT.

Figure 67 Example Message Exchange between Computer and an ANT



PPP Data Connection

The PPP frames are tunneled between the PNS and PAC over GRE (General Routing Encapsulation, RFC 1701, 1702). The individual calls within a tunnel are distinguished using the Call ID field in the GRE header.

Appendix C
Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

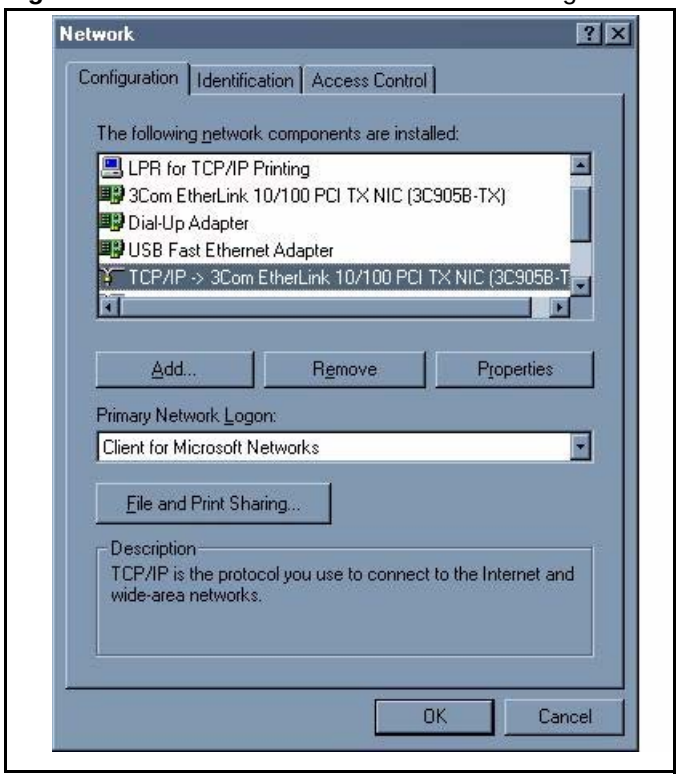
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the P-330W's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window

Figure 68 WIndows 95/98/Me: Network: Configuration



Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1. In the **Network** window, click **Add**.
2. Select **Adapter** and then click **Add**.
3. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1. In the **Network** window, click **Add**.
2. Select **Protocol** and then click **Add**.
3. Select **Microsoft** from the list of **manufacturers**.
4. Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

1. Click **Add**.
2. Select **Client** and then click **Add**.

3 Select **Microsoft** from the list of manufacturers.

4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

5 Restart your computer so the changes you made take effect.

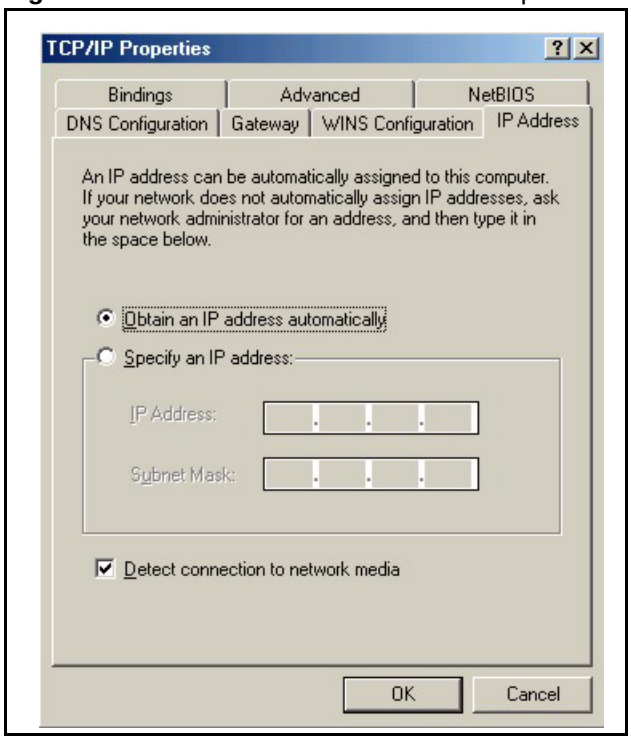
Configuring

1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**

2 Click the **IP Address** tab.

- If your IP address is dynamic, select **Obtain an IP address automatically**.
- If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

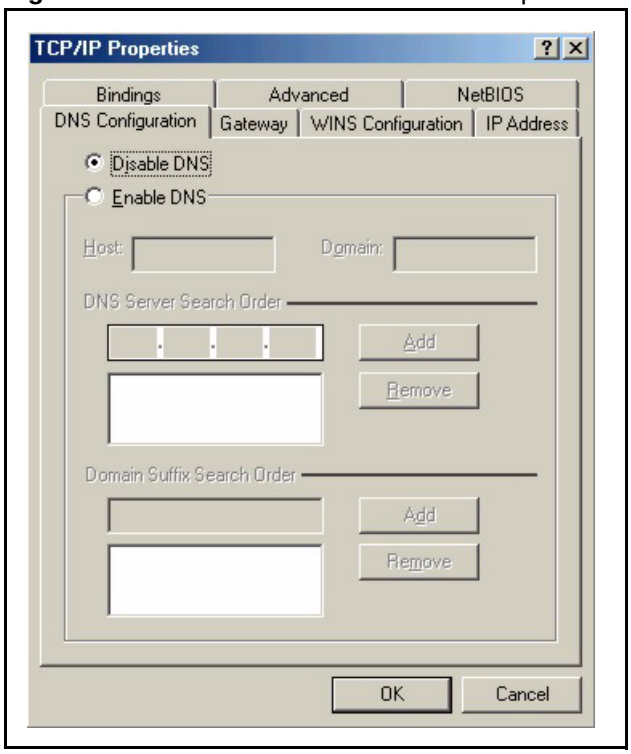
Figure 69 Windows 95/98/Me: TCP/IP Properties: IP Address


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
Detect connection to network media
OK
Cancel

3 Click the **DNS** Configuration tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 70 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



4 Click the **Gateway** tab.

- If you do not know your gateway's IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

5 Click **OK** to save and close the **TCP/IP Properties** window.

6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7 Turn on your P-330W and restart your computer when prompted.

Verifying Settings

1 Click **Start** and then **Run**.

2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

1 For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

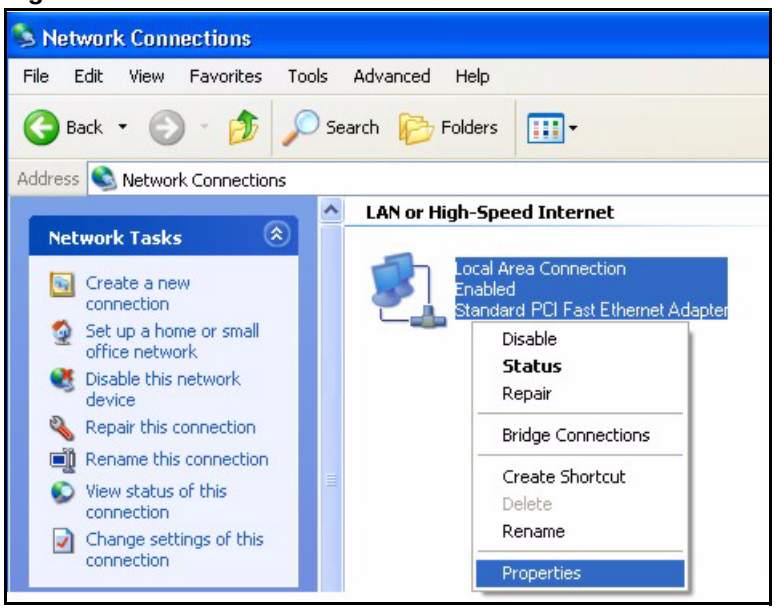
Figure 71 Windows XP: Start Menu

2 For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

Figure 72 Windows XP: Control Panel

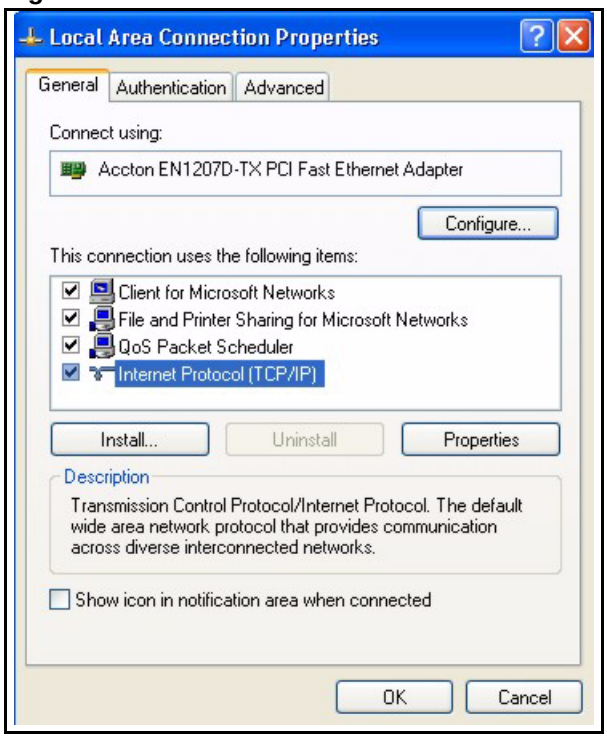
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 73 Windows XP: Control Panel: Network Connections: Properties



4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and click **Properties**.

Figure 74 Windows XP: Local Area Connection Properties

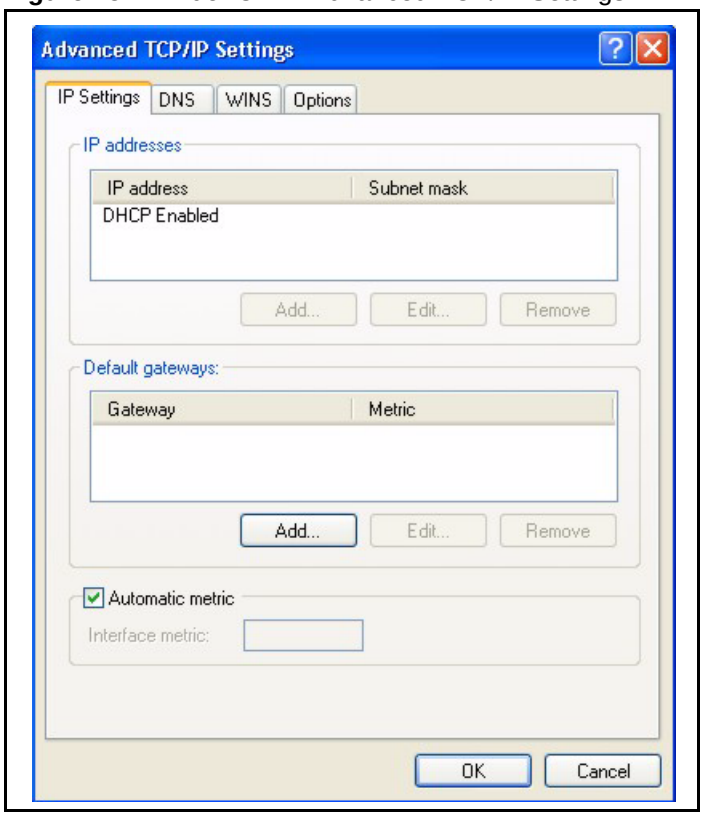

Local Area Connection Properties
General Authentication Advanced
Connect using:
Accton EN1207D-TX PCI Fast Ethernet Adapter
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol (TCP/IP)
Install... Uninstall Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
OK Cancel

5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.

- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields. Click **Advanced**.

Figure 75 Windows XP: Advanced TCP/IP Settings



6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Setting**s tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

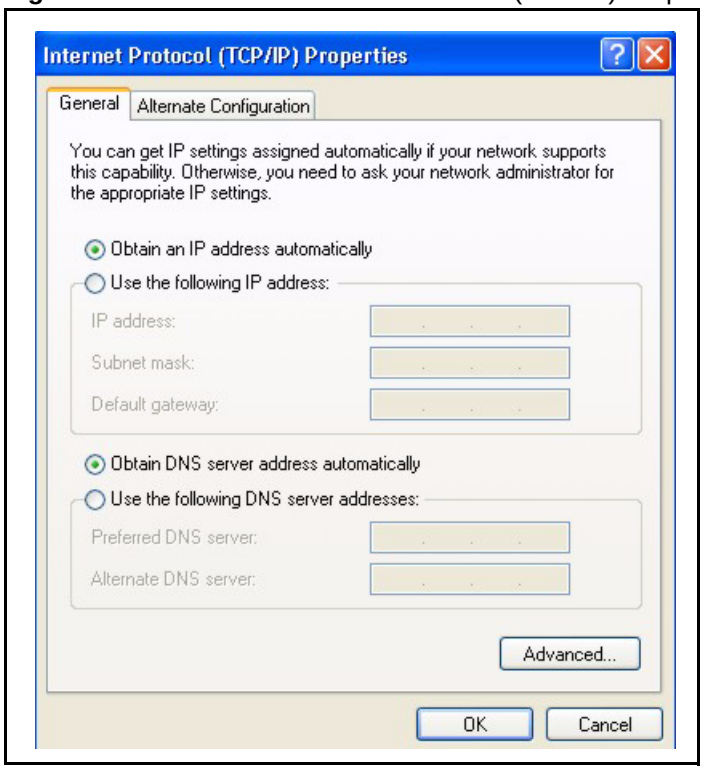
- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

7 In the **Internet Protocol TCP/IP Properties** window (the **General tab** in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 76 Windows XP: Internet Protocol (TCP/IP) Properties


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **OK** to close the **Local Area Connection Properties** window.

10 Turn on your P-330W and restart your computer (if prompted).

Verifying Settings

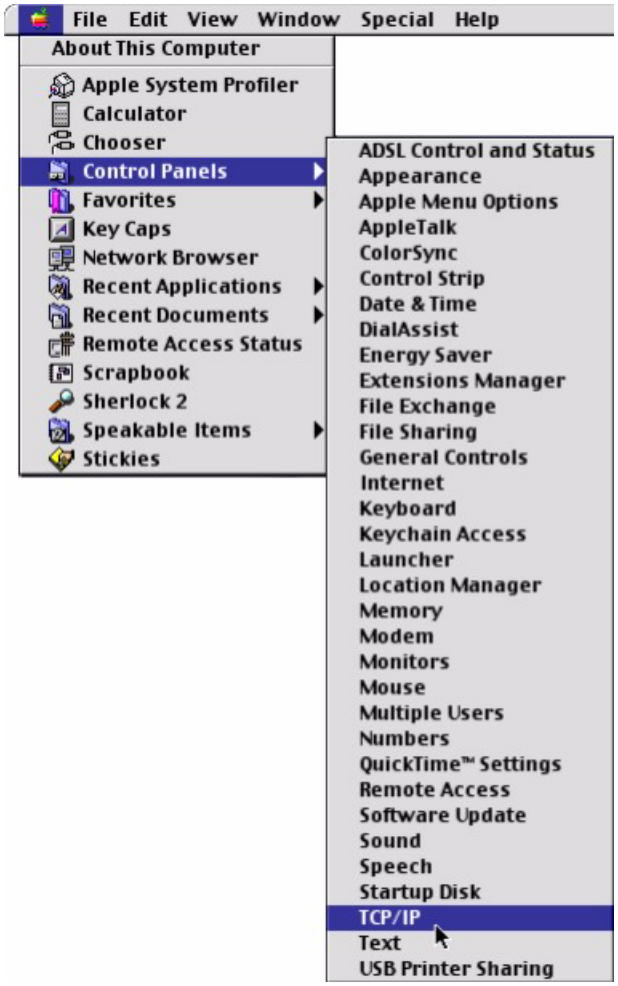
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

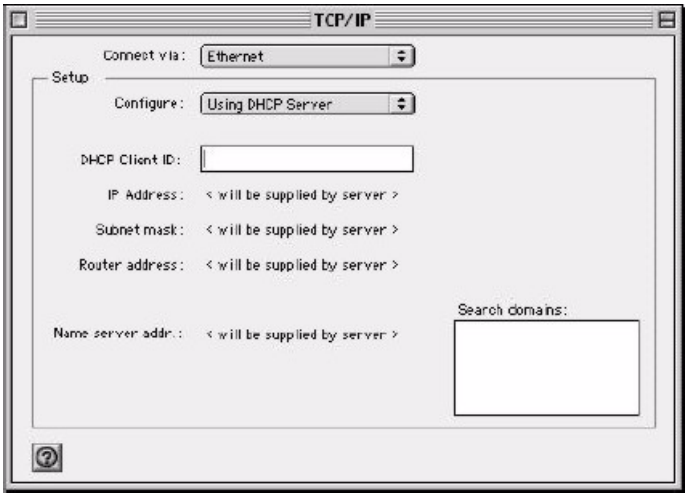
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 77 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 78 Macintosh OS 8/9: TCP/IP



3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your P-330W in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your P-330W and restart your computer (if prompted).

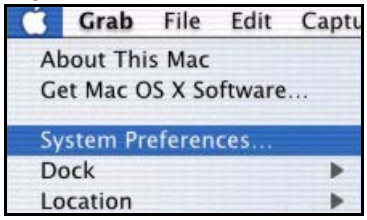
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 79 Macintosh OS X: Apple Menu



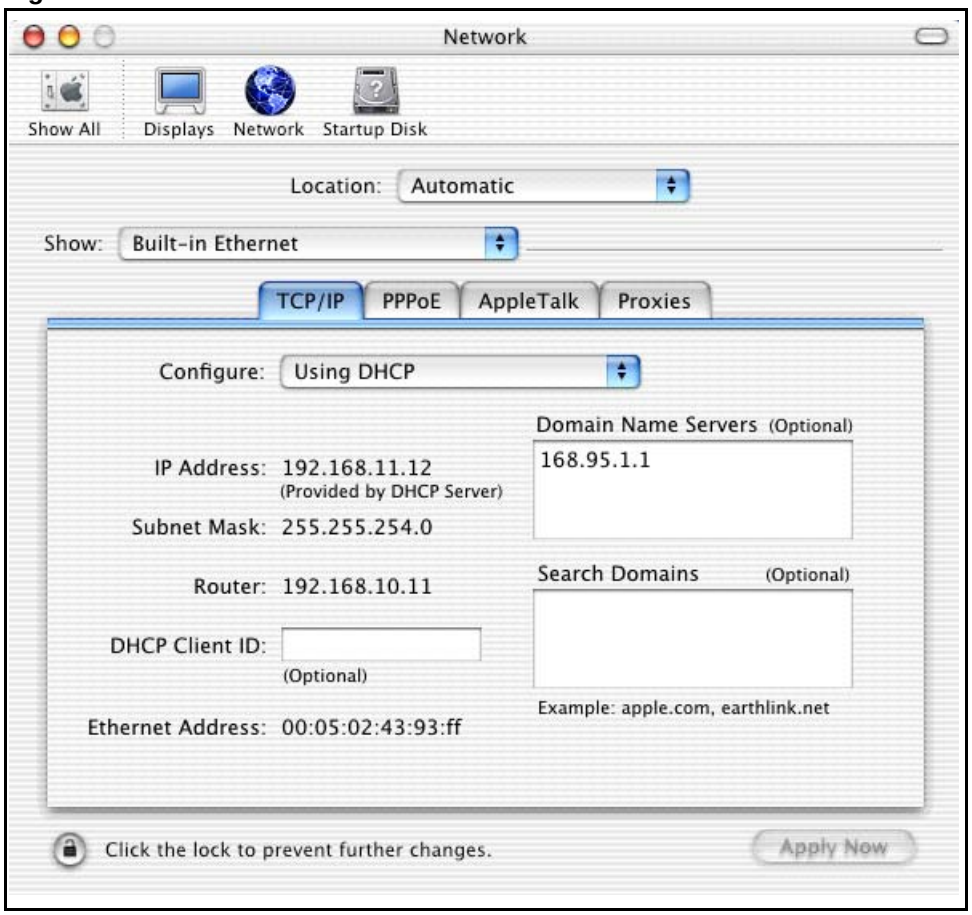
2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.

- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 80 Macintosh OS X: Network



4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your P-330W in the **Router address** box.

5 Click **Apply Now** and close the window.

6 Turn on your P-330W and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Appendix D
Wireless LAN and IEEE 802.11

A wireless LAN (WLAN) provides a flexible data communications system that you can use to access various services (navigating the Internet, email, printer services, etc.) without the use of a cabled connection. In effect a wireless LAN environment provides you the freedom to stay connected to the network while roaming around in the coverage area.

Benefits of a Wireless LAN

Wireless LAN offers the following benefits:

- It provides you with access to network services in areas otherwise hard or expensive to wire, such as historical buildings, buildings with asbestos materials and classrooms.
- It provides healthcare workers like doctors and nurses access to a complete patient's profile on a handheld or notebook computer upon entering a patient's room.
- It allows flexible workgroups a lower total cost of ownership for workspaces that are frequently reconfigured.
- It allows conference room users access to the network as they move from meeting to meeting, getting up-to-date access to information and the ability to communicate decisions while "on the go".
- It provides campus-wide networking mobility, allowing enterprises the roaming capability to set up easy-to-use wireless networks that cover the entire campus transparently.

IEEE 802.11

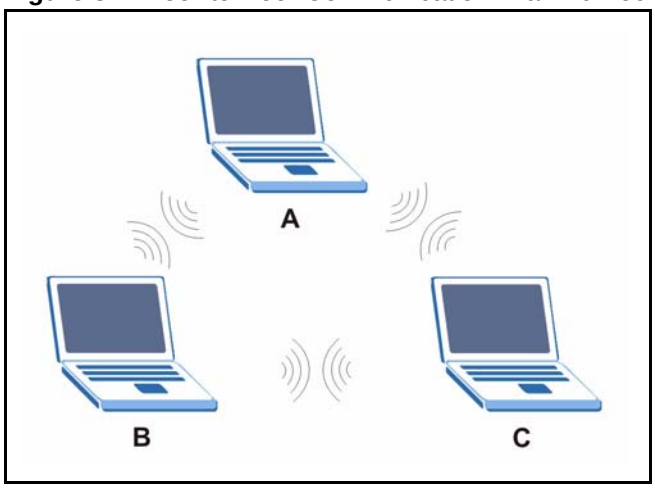
The 1997 completion of the IEEE 802.11 standard for wireless LANs (WLANs) was a first important step in the evolutionary development of wireless networking technologies. The standard was developed to maximize interoperability between differing brands of wireless LANs as well as to introduce a variety of performance improvements and benefits.

The IEEE 802.11 specifies three different transmission methods for the PHY, the layer responsible for transferring data between nodes. Two of the methods use spread spectrum RF signals, Direct Sequence Spread Spectrum (DSSS) and Frequency-Hopping Spread Spectrum (FHSS), in the 2.4 to 2.4825 GHz unlicensed ISM (Industrial, Scientific and Medical) band. The third method is infrared technology, using very high frequencies, just below visible light in the electromagnetic spectrum to carry data.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless nodes or stations (STA), which is called a Basic Service Set (BSS). In the most basic form, a wireless LAN connects a set of computers with wireless adapters. Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an Ad-hoc wireless LAN.

Figure 81 Peer-to-Peer Communication in an Ad-hoc Network

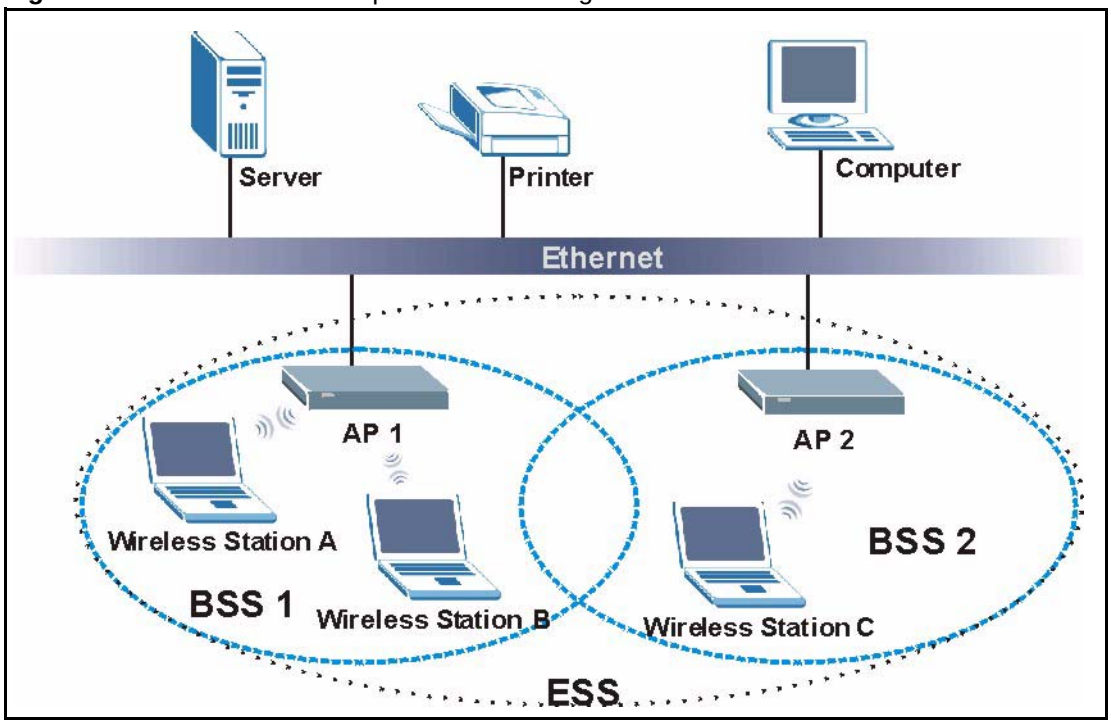


Infrastructure Wireless LAN Configuration

For Infrastructure WLANs, multiple Access Points (APs) link the WLAN to the wired network and allow users to efficiently share network resources. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood. Multiple Access Points can provide wireless coverage for an entire building or campus. All communications between stations or between a station and a wired network client go through the Access Point.

The Extended Service Set (ESS) shown in the next figure consists of a series of overlapping BSSs (each containing an Access Point) connected together by means of a Distribution System (DS). Although the DS could be any type of network, it is almost invariably an Ethernet LAN. Mobile nodes can roam between Access Points and seamless campus-wide coverage is possible.

Figure 82 ESS Provides Campus-Wide Coverage



Appendix E
Wireless LAN With IEEE 802.1x

As wireless networks become popular for both portable computing and corporate networks, security is now a priority.

Security Flaws with IEEE 802.11

Wireless networks based on the original IEEE 802.11 have a poor reputation for safety. The IEEE 802.11b wireless access standard, first published in 1999, was based on the MAC address. As the MAC address is sent across the wireless link in clear text, it is easy to spoof and fake. Even the WEP (Wire Equivalent Privacy) data encryption is unreliable as it can be easily decrypted with current computer speed

Deployment Issues with IEEE 802.11

User account management has become a network administrator's nightmare in a corporate environment, as the IEEE 802.11b standard does not provide any central user account management. User access control is done through manual modification of the MAC address table on the access point. Although WEP data encryption offers a form of data security, you have to reset the WEP key on the clients each time you change your WEP key on the access point.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices.

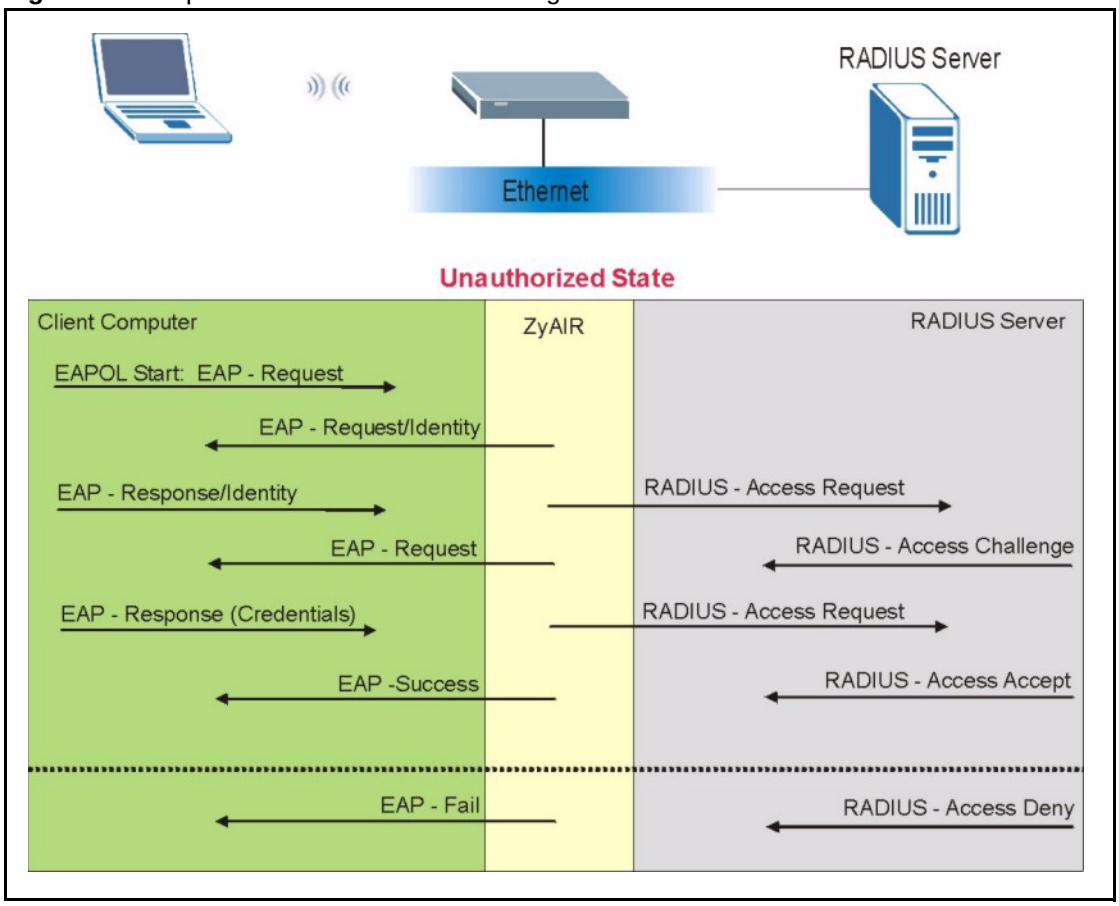
Advantages of the IEEE 802.1x

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS Server Authentication Sequence

The following figure depicts a typical wireless network with a remote RADIUS server for user authentication using EAPOL (EAP Over LAN).

Figure 83 Sequences for EAP MD5–Challenge Authentication



Appendix F
Types of EAP Authentication

This appendix discusses the five popular EAP authentication types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS**, **PEAP** and **LEAP**.

The type of authentication you use depends on the RADIUS server or the AP. Consult your network administrator for more information.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless station. The wireless station 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless stations for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

Table 48 Comparison of EAP Authentication Types

		EAP-TLS	EAP-TTLS	PEAP
Mutual Authentication	No	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional
Certificate – Server	No	Yes	Yes	Yes
Dynamic Key Exchange	No	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong
Deployment Difficulty	Easy	Hard	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes

Appendix G Antenna Selection and Positioning Recommendation

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Choosing the right antennas and positioning them properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b) or 5GHz(IEEE 802.11a) is needed to communicate efficiently in a wireless LAN.

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas For WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight. The angle of the beam width determines the direction of the coverage pattern; typically ranges from 20 degrees (less directional) to 90 degrees (very directional). The directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to –point application, position both transmitting and receiving antenna at the same height and in a direct line of sight to each other to attend the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

Index

A

Antenna
  Directional **123**
  Omni-directional **123**
Antenna gain **122**
Authentication **49**

B

Backup **87**
Basic Service Set **115**
BSS **44**, **115**

C

CA **120**
Certificate Authority **120**
Configuration **40**

D

Data Encryption **53**
Default **88**
DHCP **40**, **68**
Direct Sequence Spread Spectrum **114**
Distribution System **115**
DMZ **69**
Domain Name **70**
DS **115**
DSSS **114**
Dynamic DNS **67**, **68**

E

EAP Authentication **60**, **120**
ECHO **70**
Encryption **56**
ESS **45**, **115**
Extended Service Set **45**, **115**
Extended Service Set IDentification **48**

F

Factory LAN Defaults **40**
FHSS **114**
Finger **70**
Firewall **19**
Frequency-Hopping Spread Spectrum **114**
FTP **40**, **67**, **69**, **70**

G

General Setup **38**

H

Host **42**
HTTP **70**

I

IAPP **51**
IBSS **44**, **115**
Independent Basic Service Set **44**, **115**
IP Address **40**, **41**
IP Pool Setup **40**

L

L2TP Encapsulation **80**
LAN TCP/IP **40**

M

MAC Address Filtering **63**
MAC Filter **63**

N

NAT **70**
Network Management **70**
NNTP **70**

P

Password **41**
Point-to-Point Tunneling Protocol **70**, **78**
POP3 **70**
Port Forwarding **69**
Port Numbers **70**
PPPoE **96**
PPTP **70**
Preamble Mode **50**

R

RADIUS **59**
Related Documentation **16**
Restore **87**
RF signals **114**
RTS Threshold **46**

S

Security Parameters **53**
Service Set **48**
Services **70**
SMTP **70**
SNMP **70**
SUA **70**
Subnet Mask **40**, **41**
Syntax Conventions **16**

U

User Authentication **56**
User Name **68**

V

Virtual Servers **69**
VPN **78**, **80**

W

WEP **53**
WEP Encryption **54**, **55**, **58**
Wireless LAN **114**
Wireless Security **51**
WLAN **114**
WPA **56**
WPA with RADIUS Application **60**
WPA2 **57**
WPA-PSK Application **57**